Das Zehnte Hilbertsche Problem

Diplomarbeit

von

Franz Mauch

Universität Konstanz
Juni 1992

1. Gutachter: Prof. Dr. V. Strassen
2. Gutachter: Prof. Dr. W. Baur

Kurzer Überblick

Diese Arbeit gibt eine Darstellung der Lösung des Zehnten Hilbertschen Problems. Als Grundlage diente die Arbeit von J. P. Jones und Y. V. Matijasevič.

Zentraler Punkt meiner Arbeit ist der Nachweis der Diophantizität der Exponentialfunktion. Die Beweistechnik zum wesentlichsten Punkt, dem Übergang von der Lösungsmenge der Pellschen Gleichung zu Funktionen, die sich ähnlich wie Exponentialfunktionenen verhalten, wird zuerst an einem Analogon entwickelt: Die Diophantizität der Relation „y ist eine Potenz von x" impliziert die Diophantizität der Funktion $f(x,n) := x^n$. Der hier erhaltene Beweis wird dann auf die Lösungen der Pellschen Gleichung übertragen. Dieses Vorgehen führt zu einem tieferen Verständnis des Beweises zur Diophantizität der Exponentialfunktion.

Inhaltsverzeichnis

Einleitung

Im Jahre 1900 stellte Hilbert auf dem Internationalen Mathematiker–Kongreß eine Liste von 23 ungelösten Problemen vor, die seiner Meinung nach die Mathematik des 20. Jahrhunderts prägen würden. Das zehnte dieser Probleme war die Frage nach einem allgemeinen Verfahren zur Entscheidung, ob eine gegebene diophantische Gleichung Lösungen hat oder nicht. Es ist nicht ganz klar, ob Hilbert selbst der Überzeugung war, daß ein solches Verfahren existiert. Lange Zeit wurde vergeblich nach einem derartigen Verfahren gesucht, bis sich eine — im Sinne der Problemstellung unerwartete — Lösung ergab.

Tatsächlich dauerte es nach 1900 noch einige Zeit, bis überhaupt die Grundlagen für eine negative Beantwortung des Problems, d. h. der Feststellung, daß ein solches Verfahren nicht existieren kann, geschaffen waren. Erst mit Gödel kamen in den 20er Jahren erste Aussagen der Mathematik über ihre eigenen Möglichkeiten auf, die den Mathematikern gewisse Grenzen wiesen und eine neue Zeit einläuteten.[1]

Für die negative Lösung des Zehnten Hilbertschen Problems mußte zuerst eine Möglichkeit geschaffen werden, die es erlaubt, jedes „denkbare“ Verfahren in ein mathematisch beschreibbares umzuwandeln. Tatsächlich fand man mehrere Zugänge zu diesem Problem, u. a. die Turing–Maschine, die Registermaschine und die rekursiven Funktionen. Diese Zugänge erwiesen sich alle als äquivalent in dem Sinne, daß sie dieselbe Funktionenklasse — die von diesen Verfahren berechenbaren Funktionen — beschreiben. Anders ausgedrückt: eine von dem einen Verfahren berechenbare Funktion läßt sich auch mit den anderen Verfahren berechnen, z. B. ist eine rekursive Funktion auch turingberechenbar und umgekehrt.

Church behauptete als erster, daß diese Funktionenklasse alle „intuitiv“ berechenbare Funktionen — was man sich darunter vorzustellen hat, sei dahingestellt — abdeckt. Diese Behauptung ist bekannt als Churche These und wird allgemein akzeptiert. Man bezeichnet die obige Funktionenklasse daher schlicht als die der berechenbaren Funktionen. Wie auch in dieser Arbeit sind die Begriffe wie „berechenbar“ oder „entscheidbar“ dann immer im Sinne der Churchen These gemeint.[2]

---

[1] Eigenartigerweise wurden etwa in derselben Zeit auch für die Physiker ganz praktische Grenzen ihrer wesentlichsten Grundlage, der Messung, sichtbar. Denn die in dieser Zeit entwickelte Quantenmechanik zeigte, daß nicht alles beliebig genau meßbar ist.

[2] Man muß natürlich hinzufügen, daß innerhalb der Mathematik keine Möglichkeit besteht, zu beweisen, daß alles was der Intuition z. B. eines Mathematikers entspringen kann, auch z. B. von einer Turing-Maschine bewerkstelligt werden kann. Dieses Problem läßt sich letztlich auf ein physikalisches zurückführen, wenn man unterstellt, daß sowohl Mensch als auch Maschine den physikalischen Gesetzen gehorchen müssen.

Man stelle sich z. B. in unserem Fall der diophantischen Gleichungen, deren Lösbarkeit, wie in dieser Arbeit gezeigt wird, nicht generell entscheidbar ist, ein physikalisches System vor, das es ermöglicht, eine diophantische Gleichung in eine Anordnung von Atomen zu übersetzen, die genau dann resoniert, wenn die diophantische Gleichung eine Lösung hat. Mittels dieses Systems ist eine Entscheidung über die Lösbarkeit einer diophantischen Gleichung möglich (und damit mittels der in dieser Arbeit bewiesenen Sätze auch die Entscheidbarkeit aller aufzählbaren Mengen). Daß es ein solches System nicht gibt, kann natürlich nur im Rahmen eines physikalischen Modells gezeigt werden, nicht aber generell. (Die Existenz eines solchen Systems hätte die Aufhebung der Churchen

Es ließ sich nun mit der Berechnungstheorie zeigen, daß es Teilmengen der natürlichen Zahlen gibt, die zwar aufzählbar sind (d. h. mit einem Algorithmus können die Zahlen einer solchen Teilmenge alle nacheinander — aber nicht unbedingt in der natürlichen Reihenfolge — erzeugt werden), für die sich aber dennoch i. A. nicht entscheiden läßt (im Sinne der Churchen These), ob eine gegebene Zahl darin enthalten ist.

Martin Davis, Hilary Putnam und Julia Robinson zeigten eine Entsprechung zwischen aufzählbaren Mengen und sogenannten exponentiell–diophantischen Gleichungen, bei denen gegenüber den diophantischen Gleichungen auch Unbekannte im Exponenten zugelassen sind. Daraus ergibt sich, daß die Lösbarkeit exponentiell–diophantischer Gleichungen i. a. unentscheidbar ist.

Matijasevič bewies schließlich in [2], daß die Exponentialfunktion selbst diophantisch ist, und zeigte damit die Identität der Menge der aufzählbaren Mengen mit der der diophantischen Mengen. Die Existenz von aufzählbaren aber nicht entscheidbaren Mengen liefert dann den Schluß, daß kein Verfahren (im Sinne der Churchen These) zur Lösung des Zehnten Hilbertschen Problems existiert.

Diesem letzten Schritt gilt das Hauptinteresse unserer Arbeit. Er wird in Kapitel 2 dargestellt werden. Ausgehend von der Annahme, daß die Relation „y ist eine Potenz von x“ diophantisch ist, werden wir die Diophantizität der Exponentialfunktion zeigen. Dann werden wir Analoga unserer technischen Einzelschritte bei den Lösungen der Pellschen Gleichung herleiten, die uns dann die Lemmata liefern, die auch Matijasevič in seinem dieser Arbeit zugrunde liegenden Artikel [1] verwendet hat, aber hier mit vielleicht instruktiveren Beweisen. Ebenso werden sich dadurch die Beweisideen aus der technischen Beweisführung klarer herausheben.

Dem historisch früheren Teil der Lösung, allerdings in einer neueren und wohl kürzesten bekannten Variante mittels Registermaschinen, entnommen aus [1], ist Kapitel 3 gewidmet. Mit der in Kapitel 2 gezeigten Diophantizität der Exponentialfunktion können wir die Diophantizität der berechenbaren Funktionen zeigen.

Diesen beiden Kapiteln liegt Kapitel 1 zur Erklärung der Begriffe und zum Nachweis der Diophantizität einiger bekannter Relationen, die wir in den weiteren Schritten benötigen, zugrunde. Dann werden wir die Lösung des Zehnten Hilbertschen Problems darstellen und den Beweis bis auf das erst in Kapitel 3 gezeigte Korollar angeben.

Die wesentliche Änderung gegenüber dem Beweis der Vorlage [1] besteht in den Abschnitten 2.2, 2.3 und 2.4. Alle anderen Abschnitte sind mehr oder weniger veränderte Übernahmen aus der Literatur.

These als Konsequenz, da eine einschränkende Erklärung der Bezeichnung „intuitiv berechenbar“ die Churche These ziemlich inhaltlos machen würde.

Kapitel 1

Grundlagen

1.1 Diophantische Mengen und Funktionen

Bezeichnung 1.1.1 *Wir bezeichnen mit* $\mathbb{N}$ *die natürlichen Zahlen und mit* $\mathbb{N}_0$ *die nichtnegativen ganzen Zahlen, also* $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Bezeichnung 1.1.2 *Sei* $n \in \mathbb{N}$ *und* $A \subset \mathbb{N}_0^n$. *Dann schreiben wir für* $(a_1, \ldots, a_n) \in A$ *kurz* $A(a_1, \ldots, a_n)$. *In dieser Form faßt man* A *auch als Relation auf.*

Mit diesen Bezeichnungen können wir den Begriff der diophantischen Menge definieren.

Definition 1.1.3 *Sei* $n \in \mathbb{N}$ *und* $A \subset \mathbb{N}_0^n$. *Wir nennen* A *diophantisch genau dann, wenn ein* $m \in \mathbb{N}_0$ *und ein Polynom* $P \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ *existiert,*[1] *so daß*

$$A(a_1, \ldots, a_n) \iff \exists x_1, \ldots, x_m \in \mathbb{N}_0 \quad \text{mit} \quad P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\,. \tag{1.1}$$

Man bezeichnet $a_1, \ldots, a_n$ *als Parameter und* $x_1, \ldots, x_n$ *als Unbekannte, außerdem bezeichnet man die Gleichung* $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ *für die Unbekannten* $x_1, \ldots, x_m$ *als diophantische Gleichung (d. h. die* $a_1, \ldots, a_n$ *parametrisieren diophantische Gleichungen).*

Man beachte, daß sowohl für die Parameter als auch für die Lösungen nichtnegative ganze Zahlen gefordert werden, jedoch die Polynomkoeffizienten selbst ganze Zahlen sein dürfen. Diese Willkür ist aber für unser Problem nicht wesentlich, was wir im Anhang unter A.1 ausführen werden.
Wir benötigen im weiteren den Begriff einer diophantischen Funktion.

Definition 1.1.4 *Seien* $m, n \in \mathbb{N}$. *Eine Funktion* $f : \mathbb{N}_0^m \to \mathbb{N}_0^n$ *heißt diophantisch genau dann, wenn* $\operatorname{graph}(f) \subset \mathbb{N}_0^{m+n}$ *diophantisch ist.*

Die Frage, ob die diophantische Gleichung mit einem bestimmten $a \in \mathbb{N}_0^n$ als Parameter eine Lösung besitzt, ist äquivalent zur Frage, ob „$a \in A$". Mit Hilfe der Definition 1.1.3 läßt sich damit das Hilbertsche Problem so formulieren: Läßt sich für jede diophantische Menge $A \subset \mathbb{N}_0^n$ und $a \in \mathbb{N}_0^n$ „entscheiden", ob $a \in A$? Dabei ist das „entscheiden" i. S. der Existenz eines Algorithmus, der die Antwort liefert, gemeint. Diese ungenaue Formulierung soll nun im nächsten Abschnitt im Rahmen der Berechnungstheorie konkretisiert werden.

[1] Entsprechend den allgemeinen Bezeichnungen seien hier und im weiteren im Falle $m = 0$ die Ausdrücke mit $x_1, \ldots, x_m$ einfach wegzulassen. Eine gesonderte Behandlung dieses Falles würde die Formulierung unverhältnismäßig aufblähen.

1.2 Grundlagen aus der Berechnungstheorie[2]

Die Theorie der Berechenbarkeit von Funktionen gibt verschiedene Möglichkeiten zur Definition von (total) berechenbaren Funktionen. So werden u. a. definiert: Turingberechenbarkeit, μ–Rekursivität, Berechenbarkeit durch Registermaschinen. Es hat sich aber gezeigt, daß all diese Definitionen äquivalent sind und auch weitere Überlegungen zu keinem Berechenbarkeitsbegriff geführt haben, der mehr Funktionen umfaßt. Die Churche These sagt aus, daß die durch all diese äquivalenten Begriffe definierte Menge generell alle „intuitiv" berechenbaren Funktionen umfaßt. Diese These wird heute allgemein akzeptiert.

Im folgenden sind die für uns interessanten Bezeichnungen und Sätze aus der Berechnungstheorie ohne Beweise zusammengestellt.

Bezeichnung 1.2.1 *Wir bezeichnen eine turingberechenbare bzw. μ-rekursive Funktion usw. kurz als berechenbar.*

Bemerkung 1.2.2 *Man beachte, daß unter Berechenbarkeit immer totale Berechenbarkeit verstanden wird, das heißt z. B., daß die Turingmaschine, die eine turingberechenbare Funktion realisiert, bei jedem legalen[3] Input stehen bleibt. Dagegen bezeichnet man Funktionen, die nicht notwendig überall berechenbar sind, als partiell berechenbar. Da solche Funktionen hier nicht benötigt werden, sollte diese Bemerkung als Abgrenzung der berechenbaren Funktionen von den partiell berechenbaren ausreichen.*

Definition 1.2.3 *Sei $m, n \in \mathbb{N}$. Wir bezeichnen mit $B_{m,n}$ die Menge aller (total) berechenbaren Funktionen $f : \mathbb{N}_0^m \to \mathbb{N}_0^n$.*

Definition 1.2.4 *Sei $n \in \mathbb{N}$. Eine Menge $A \subset \mathbb{N}_0^n$ heißt aufzählbar genau dann, wenn $A = \{\}$ oder $\exists m \in \mathbb{N}, f \in B_{m,n}$ mit $A = \mathrm{im}(f)$.*

Definition 1.2.5 *Sei $n \in \mathbb{N}$. Eine Menge $A \subset \mathbb{N}_0^n$ heißt entscheidbar genau dann, wenn für ihre charakteristische Funktion I_A gilt $I_A \in B_{n,1}$.*

Zur Verbindung der beiden Begriffe folgendes Lemma, welches nicht sehr tiefgründig ist.

Lemma 1.2.6 *Für $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$ gilt:*

$$A \text{ entscheidbar} \iff A \text{ und } \mathbb{N}_0^n \backslash A \text{ aufzählbar}. \tag{1.2}$$

Ein für uns wesentlicher Satz aus der Berechnungstheorie lautet

Satz 1.2.7 *Es existiert ein $A \subset \mathbb{N}_0$ aufzählbar, aber nicht entscheidbar.*

Da wir bei der Definition diophantischer Funktionen auf deren Graphen zurückgriffen, wollen wir auch die Verbindung zwischen der Berechenbarkeit einer Funktion und der Entscheidbarkeit bzw. Aufzählbarkeit seines Graphen aufzeigen.

Satz 1.2.8 *Sei $m, n \in \mathbb{N}$ und $f : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^n$. Dann gilt*

$$f \in B_{m,n} \iff \mathrm{graph}(f) \text{ entscheidbar} \iff \mathrm{graph}(f) \text{ aufzählbar}. \tag{1.3}$$

Die zunächst erstaunliche Äquivalenz der Entscheidbarkeit und der Aufzählbarkeit bei Graphen von Funktionen, ergibt sich aus der speziellen Struktur eines Graphen.

[2] Diesem Abschnitt liegt als Literatur vornehmlich [5] zugrunde.

[3] Da wir hier nicht zu sehr auf Turingmaschinen eingehen wollen, sei dieser Begriff nicht näher erläutert

Für den nächsten Abschnitt benötigen wir die Berechenbarkeit einiger einfacher Funktionen.

Bemerkung 1.2.9 *(i) Die konstanten Funktionen und die Projektionen sind berechenbar.*

(ii) Für $A = \{0\}$ ist I_A berechenbar, d. h. A entscheidbar.

(iii) Die nichtnegativwertigen Polynome aus $\mathbb{Z}[x_1, \dots, x_n]$ mit $n \in \mathbb{N}$ als Funktionen $\mathbb{N}_0^n \longrightarrow \mathbb{N}_0$ sind berechenbar. (Der Ausschluß von Polynomen, die auf $\mathbb{Z}^n$ negative Werte annehmen können, ist nötig aufgrund der Restriktion auf Funktionen $\mathbb{N}_0^n \longrightarrow \mathbb{N}_0$ in der Definition diophantischer Funktionen.)

(iv) Die Verkettung, (komponentenweise) Addition und (skalare) Multiplikation berechenbarer Funktionen liefern wieder berechenbare Funktionen.

1.3 Die Formulierung und Lösung des Zehnten Hilbertschen Problems

Mit Hilfe der zwei vorgehenden Abschnitte sind wir nun in der Lage, das Zehnte Hilbertsche Problem exakt zu formulieren und den Satz, der die Lösung direkt impliziert, anzugeben. Der Beweis dieses Satzes aber wird fast den ganzen Rest dieser Arbeit in Anspruch nehmen.

In der Formulierung von Hilbert wurde ein Algorithmus gesucht, mit Hilfe dessen sich entscheiden läßt, ob eine gegebene diophantische Gleichung eine Lösung besitzt oder nicht. Da man diesen Algorithmus nicht fand, fragte man sich, ob ein solcher Algorithmus überhaupt existiert. Mit Hilfe von Definition 1.1.3 läßt sich diese Frage so formulieren: Folgt aus $A \in \mathbb{N}_0^n$ diophantisch, daß A entscheidbar. Tatsächlich werden wir aber den folgenden Satz zeigen:

Satz 1.3.1 *Sei $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$, dann gilt*

$$A \text{ diophantisch} \iff A \text{ aufzählbar}. \tag{1.4}$$

Beweis :

„⇒“: Mit Hilfe der Bemerkung 1.2.9 läßt sich der Beweis einfach vollziehen.

Für $A = \{\}$ ist nach Definition von Aufzählbarkeit nichts zu beweisen.

Sei also $A \neq \{\}$. Dann existiert $(b_1, \dots, b_n) \in A$. Weiterhin sei A diophantisch mittels des Polynoms $P \in \mathbb{Z}[a_1, \dots, a_n, x_1, \dots, x_m]$. Wir definieren dann $f : \mathbb{N}_0^{n+m} \longrightarrow \mathbb{N}_0^n$ durch:

$$\begin{aligned} &f(a_1, \dots, a_n, x_1, \dots, x_m) := \\ &\quad (b_1, \dots, b_n) + I_{\{0\}}(P(a_1, \dots, a_n, x_1, \dots, x_m)^2)((a_1, \dots, a_n) - (b_1, \dots, b_n)) . \end{aligned}$$

Wegen Bemerkung 1.2.9 ist f berechenbar. Weiterhin ist $f(\mathbb{N}_0^{n+m}) \subset A$. Denn $f(a_1, \dots, a_n, x_1, \dots, x_m)$ ist entweder $(a_1, \dots, a_n)$ oder $(b_1, \dots, b_n)$. Nun ist $(b_1, \dots, b_n) \in A$, und $(a_1, \dots, a_n)$ erhalten wir nur, wenn $P(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ und damit $(a_1, \dots, a_n) \in A$.

Ist umgekehrt $(a_1, \dots, a_n) \in A$, so $\exists x_1, \dots, x_n \in \mathbb{N}_0$ mit $P(a_1, \dots, a_n, x_1, \dots, x_m) = 0$, dann ist aber $f(a_1, \dots, a_n, x_1, \dots, x_m) = (a_1, \dots, a_n)$ und damit $(a_1, \dots, a_n) \in f(\mathbb{N}_0^{n+m})$. Also ist $A \subset f(\mathbb{N}_0^{n+m})$.

Damit folgt $f(\mathbb{N}_0^{n+m}) = A$, und da f berechenbar, folgt damit daß A aufzählbar ist.

„⇐“: Dies ist der schwierige Teil des Beweises. Allerdings wird die Hauptarbeit auf Satz 1.3.3 abgewälzt, mit dem wir dann die Implikation am Ende dieses Abschnitts beweisen werden.

Mit Hilfe der nächsten zwei Kapitel wird dann der Satz 1.3.3 am Ende von Kapitel 3 bewiesen werden und damit auch der vorstehende Satz vollständig bewiesen sein.

□

Der gelieferte erste Teil des Beweises ist eine formale Darstellung des einfachen Algorithmuses, der die gesuchte Funktion f mit $\mathrm{im}(f) = A$ liefert: „Setze nacheinander alle Möglichkeiten für a und x in P ein; wenn du 0 erhältst, merke dir a.“ Dann erhält man letztlich auch alle Parameter, bei denen die diophantische Gleichung eine Lösung besitzt, also A.

Aus dem Satz 1.3.1 läßt sich mittels Satz 1.2.7 das folgende Korollar ziehen, das gleichzeitig die oben gestellte Frage beantwortet.

Korollar 1.3.2 *Es existiert eine diophantische, aber nicht entscheidbare Menge.*

Beweis :

Die Menge A aus dem Satz 1.2.7 ist aufzählbar, aber nicht entscheidbar. Wegen Satz 1.3.1 ist A damit diophantisch, aber nicht entscheidbar. □

Es ist zu bemerken, daß nur eine Implikation des Satzes 1.3.1 verwendet wurde, und zwar die schwierigere und noch nicht bewiesene Implikation, deren Beweis der wesentliche Bestandteil dieser Arbeit ist.

Wir wollen die nichtbewiesene Implikation des Satzes 1.3.1 mittels einer der beiden Implikationen des folgenden Satzes beweisen, welche selbst erst später bewiesen wird.

Satz 1.3.3 *Sei $m, n \in \mathbb{N}$ und $f : \mathbb{N}^m \longrightarrow \mathbb{N}^n$. Dann gilt*

$$f \text{ diophantisch} \iff f \text{ berechenbar}. \tag{1.5}$$

Beweis :

„⇒“: Aus f diophantisch folgt $\mathrm{graph}(f)$ diophantisch. Aus der bewiesenen Implikation von 1.3.1 folgt, daß $\mathrm{graph}(f)$ aufzählbar ist, und wegen Satz 1.2.8 ist damit f berechenbar.

„⇐“: s. 3.3.1

□

Beweis von Satz 1.3.1, „⇐“:

Aus A aufzählbar folgt die Existenz einer berechenbaren Funktion f mit $A = \mathrm{im}(f)$. Aufgrund der bewiesenen Implikation „⇒“ des Satzes 1.3.3 ist f damit auch diophantisch und damit $\mathrm{graph}(f)$ diophantisch. A ist wegen $A = \mathrm{im}(f)$ die Projektion von f auf die Bildkoordinaten und damit wegen Lemma 1.4.5, das ohne Verwendung dieses Abschnitts im nächsten Abschnitt dargestellt und bewiesen wird,[4] auch diophantisch. □

Damit bleibt uns also noch der Beweis von 1.3.3„⇐“, für den die nächsten zwei Kapitel benötigt werden.

[4]Zur besseren Strukturierung wurde eine Vorwärtsreferenz einer Umstellung vorgezogen.

1.4 Hilfssätze über Diophantische Relationen

Lemma 1.4.1 *Die Relationen* $=, \leq, <, \mid$ *auf* $\mathbb{N}_0 \times \mathbb{N}_0$ *sind diophantisch.*

Beweis :

„=“: Setze $P(a_1, a_2) := a_1 - a_2 \in \mathbb{Z}[a_1, a_2]$. Dann ist $P(a_1, a_2) = 0 \iff a_1 - a_2 = 0 \iff a_1 = a_2$.

„≤“: Setze $P(a_1, a_2, x) := a_1 - a_2 + x \in \mathbb{Z}[a_1, a_2, x]$. Dann ist $\exists x \in \mathbb{N}_0 : P(a_1, a_2, x) = 0 \iff \exists x \in \mathbb{N}_0 : a_1 - a_2 + x = 0 \iff a_1 \leq a_2$.

„<“: Setze $P(a_1, a_2, x) := a_1 - a_2 + 1 + x \in \mathbb{Z}[a_1, a_2, x]$. Dann ist $\exists x \in \mathbb{N}_0 : P(a_1, a_2, x) = 0 \iff \exists x \in \mathbb{N}_0 : a_1 - a_2 + 1 + x = 0 \iff a_1 < a_2$.

„|“: Setze $P(a_1, a_2, x) := a_1 x - a_2 \in \mathbb{Z}[a_1, a_2, x]$. Dann ist $\exists x \in \mathbb{N}_0 : P(a_1, a_2, x) = 0 \iff \exists x \in \mathbb{N}_0 : a_2 = x a_1 \iff a_1 | a_2$.

□

Lemma 1.4.2 *Sei* $n \in \mathbb{N}$ *und* $A \subset \mathbb{N}_0^n$ *diophantisch. Sei* σ *eine Permutation der Zahlen* $1, \ldots, n$ *(d. h.* $\sigma \in S_n$*) und sei* $B \subset \mathbb{N}_0^n$ *durch*

$$B(a_1, \ldots, a_n) \quad :\iff \quad A(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) . \tag{1.6}$$

definiert. Dann ist auch B *diophantisch.*

Beweis :

Nach Definition existieren $m \in \mathbb{N}_0$ und $P(a_1, \ldots, a_n, x_1, \ldots, x_m) \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$. Sei $Q(a_1, \ldots, a_n, x_1, \ldots, x_m) := P(a_{\sigma(1)}, \ldots, a_{\sigma(n)}, x_1, \ldots, x_m)$. Damit ist $Q \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_n]$. Dann gilt

$$\begin{aligned} B(a_1, \ldots, a_n) &\iff A(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) \\ &\iff \exists x_1, \ldots, x_m \in \mathbb{N}_0 : P(a_{\sigma(1)}, \ldots, a_{\sigma(n)}, x_1, \ldots, x_m) = 0 \\ &\iff \exists x_1, \ldots, x_m \in \mathbb{N}_0 : Q(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 . \end{aligned}$$

Damit ist B diophantisch. □

Lemma 1.4.3 *Seien* $n, k, k' \in \mathbb{N}_0$ *und* $n + k, n + k' > 0$*. Weiterhin seien* $A \subset \mathbb{N}_0^{n+k}$ *und* $B \subset \mathbb{N}_0^{n+k'}$ *diophantisch, und seien* $a := (a_1, \ldots, a_n) \in \mathbb{N}_0^n, b := (b_1, \ldots, b_k) \in \mathbb{N}_0^k, b' := (b'_1, \ldots, b'_{k'}) \in \mathbb{N}_0^{k'}$*. Seien* $C, D \subset \mathbb{N}_0^{n+k+k'}$ *gegeben durch*

$$\begin{aligned} C(a, b, b') &:\iff A(a, b) \wedge B(a, b') , \\ D(a, b, b') &:\iff A(a, b) \vee B(a, b') . \end{aligned}$$

Dann sind C, D *diophantisch.*

Beweis :

Sei $a=(a_1,\ldots,a_n), b=(b_1,\ldots,b_k), b'=(b'_1,\ldots,b'_{k'})$. Wegen A und B diophantisch existieren $m,m'\in \mathbb{N}_0$ und $P\in \mathbb{Z}[a,b,x_1,\ldots,x_m]$ und $Q\in \mathbb{Z}[a,b',x'_1,\ldots,x'_{m'}]$ mit

$$\begin{aligned} A(a,b) &\iff \exists x_1,\ldots,x_m\in \mathbb{N}_0 : P(a,b,x_1,\ldots,x_m)=0\,,\\ B(a,b') &\iff \exists x'_1,\ldots,x'_{m'}\in \mathbb{N}_0 : Q(a,b',x'_1,\ldots,x'_{m'})=0\,. \end{aligned}$$

Sei nun $x=(x_1,\ldots,x_m)$, $x'=(x'_1,\ldots,x'_{m'})$. Wir definieren die Polynome R und S durch

$$\begin{aligned} R(a,b,b',x,x') &:= P(a,b,x)^2+Q(a,b',x')^2\,,\\ S(a,b,b',x,x') &:= P(a,b,x)Q(a,b',x')\,. \end{aligned}$$

Dann gilt $R,S\in \mathbb{Z}[a,b,b',x,x']$ und

$$\begin{aligned} C(a,b,b') &\iff A(a,b)\wedge B(a,b')\\ &\iff (\exists x\in \mathbb{N}_0^m : P(a,b,x)=0)\wedge(\exists x'\in \mathbb{N}_0^{m'} : Q(a,b',x')=0)\\ &\iff \exists x\in \mathbb{N}_0^m, x'\in \mathbb{N}_0^{m'} : P(a,b,x)^2=0\wedge Q(a,b',x')^2=0\\ &\iff \exists x\in \mathbb{N}_0^m, x'\in \mathbb{N}_0^{m'} : R(a,b,b',x,x')=0\,. \end{aligned}$$

und ebenso

$$\begin{aligned} D(a,b,b') &\iff A(a,b)\vee B(a,b')\\ &\iff (\exists x\in \mathbb{N}_0^m : P(a,b,x)=0)\vee(\exists x'\in \mathbb{N}_0^{m'} : Q(a,b',x')=0)\\ &\iff \exists x\in \mathbb{N}_0^m, x'\in \mathbb{N}_0^{m'} : P(a,b,x)=0\vee Q(a,b',x')=0\\ &\iff \exists x\in \mathbb{N}_0^m, x'\in \mathbb{N}_0^{m'} : S(a,b,b',x,x')=0\,. \end{aligned}$$

Damit sind C und D diophantisch. □

Die Trennung der Argumente von A und B in die gemeinsamen Argumente $a_1,\ldots,a_n$ und nicht gemeinsame $b_1,\ldots,b_k$ und $b'_1,\ldots,b'_{k'}$ erfolgte im Hinblick auf möglichst große Allgemeinheit.

Lemma 1.4.4 *Seien $n,k\in \mathbb{N}$ und sei $A\subset \mathbb{N}_0^{n+k}$ diophantisch und $y_1,\ldots,y_k\in \mathbb{N}_0$. Dann ist die durch*

$$B(a_1,\ldots,a_n) \quad :\iff \quad A(a_1,\ldots,a_n,y_1,\ldots,y_n) \tag{1.7}$$

definierte Relation B, die natürlich von $y_1,\ldots,y_k$ abhängt, auch diophantisch.

Beweis :

Sei $P\in \mathbb{Z}[a_1,\ldots,a_{n+k},x_1,\ldots,x_m]$ das zu A gehörige Polynom. Dann ist durch

$$Q(a_1,\ldots,a_n,x_1,\ldots,x_m):=P(a_1,\ldots,a_n,y_1,\ldots,y_k,x_1,\ldots,x_m)$$

ein Polynom aus $\mathbb{Z}[a_1,\ldots,a_n,x_1,\ldots,x_m]$ definiert, welches das zu B gehörende Polynom ist. □

Lemma 1.4.5 *Seien $n, k \in \mathbb{N}$, sei $A \subset \mathbb{N}_0^{n+k}$ diophantisch und sei $B \subset \mathbb{N}_0^n$ durch*

$$B(a_1, \ldots, a_n) :\Longleftrightarrow (\exists a_{n+1}, \ldots, a_{n+k} \in \mathbb{N}_0 : A(a_1, \ldots, a_{n+k})) \tag{1.8}$$

definiert, oder anders ausgedrückt $B := \mathrm{proj}_{1,\ldots,n} A$.
Dann ist auch B diophantisch.

Beweis :

Da A diophantisch, existiert $m \in \mathbb{N}_0$ und $P \in \mathbb{Z}[a_1 \ldots a_{n+k}, x_1, \ldots, x_m]$ mit

$$A(a_1, \ldots, a_{n+k}) \iff \exists x_1, \ldots, x_m \in \mathbb{N}_0 : P(a_1, \ldots, a_{n+k}, x_1, \ldots, x_m) = 0\,. \tag{1.9}$$

Damit ergibt sich aber sofort:

$$B(a_1, \ldots, a_n) \iff \exists a_{n+1}, \ldots, a_{n+k}, x_1, \ldots, x_m \in \mathbb{N}_0 : P(a_1, \ldots, a_{n+k}, x_1, \ldots, x_m) = 0\,, \tag{1.10}$$

und damit ist B auch diophantisch. $\square$

Daß nicht alles so einfach bei diophantischen Mengen funktioniert, zeigt die folgende Bemerkung.

Bemerkung 1.4.6

(i) Ist $A \subset \mathbb{N}_0^{n+1}$ diophantisch, so ist die durch $B(a_1, \ldots, a_n) :\Longleftrightarrow \forall a_{n+1} \in \mathbb{N}_0 : A(a_1, \ldots, a_{n+1})$ definierte Relation auf $\mathbb{N}_0^n$ nicht unbedingt auch diophantisch.[5]

(ii) Betrachten wir nun die durch

$$C(a_1, \ldots, a_n, a_{n+1}) \quad :\Longleftrightarrow \quad \bigwedge_{i=1}^{a_{n+1}} A(a_1, \ldots, a_n, i) \tag{1.11}$$

definierte Relation, so ist diese im Gegensatz zu der in (i) definierten Relation B diophantisch, jedoch benötigt man zum Beweis dieser Tatsache den Satz 1.3.1, den wir hier gerade beweisen wollen. Also läßt sich diese Tatsache hier nicht für unsere Zwecke benutzen.

(iii) Weiterhin folgt aus A diophantisch nicht $\mathbb{N}_0^{n+1} \setminus A$ diophantisch. Aus dem Gegenteil ließe sich nämlich ganz einfach folgern, daß das in (i) definierte B diophantisch wäre.

Die dargestellte Behauptung sei Warnung vor dem leichtfertigen Umgang mit Quantoren bei diophantischen Relationen.

Nach der Behandlung von Relationen nun einige Eigenschaften bei diophantischen Funktionen:

Lemma 1.4.7 *Sei $n, m, k \in \mathbb{N}$, seien $g_1, \ldots, g_n$ diophantische Funktionen $\mathbb{N}_0^m \to \mathbb{N}_0$, sei $A \subset \mathbb{N}_0^n$ eine diophantische Relation und f eine diophantische Funktion $\mathbb{N}_0^n \to \mathbb{N}_0^k$. Weiterhin sei zur Abkürzung $x = (x_1, \ldots, x_m)$.*

Dann ist auch die Funktion $h : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^k$ mit $h(x) := f(g_1(x), \ldots, g_n(x))$ und die Relation $B \subset \mathbb{N}^n$ mit $B(x) :\Longleftrightarrow A(g_1(x), \ldots, g_n(x))$ diophantisch.

[5]Tatsächlich existieren Beispiele, bei denen man durch Anwendung eines Allquantors eine nichtdiophantische Relation erhält. Genaueres s. Anhang A.2.

Beweis :

Sei $z := (z_1, \ldots, z_k)$. Es gilt

$$z = h(x) \iff \exists y_1, \ldots, y_n : \left(\bigwedge_{i=1}^{n} y_i = g_i(x) \right) \wedge (z = f(y_1, \ldots, y_n)) \,. \tag{1.12}$$

Da hier auf der rechten Seite eine konstante Anzahl von Gleichungen auftaucht, ergibt sich mit Hilfe von Lemma 1.4.3 und einfacher Induktion die Diophantizität der rechten Seite. (Zum Beweis wurde <u>nicht</u> die unbewiesene Bemerkung 1.4.6(ii), in der die Anzahl der Gleichungen als Argument der Funktion auftritt, verwendet.) □

Lemma 1.4.8 *Sei für $m \in \mathbb{N}_0$ die Funktion $f : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0$ durch ein $P \in \mathbb{Z}[x_1, \ldots, x_m]$ definiert. Dann ist f diophantisch.*

Beweis :

Setze $Q(x_1, \ldots, x_m, y) := P(x_1, \ldots, x_m) - y \in \mathbb{Z}[x_1, \ldots, x_m, y]$. Dann gilt $y = f(x_1, \ldots, x_m)$ $\iff Q(x_1, \ldots, x_m, y) = 0$. □

Lemma 1.4.9 *Sei f eine eineindeutige Funktion $\mathbb{N}_0 \to \mathbb{N}_0$. Dann gilt*

$$f \textit{ diophantisch} \iff f^{-1} \textit{ diophantisch} \,. \tag{1.13}$$

Beweis :

Es gilt

$$(x, y) \in \operatorname{graph}(f) \iff (y, x) \in \operatorname{graph}(f^{-1}) \,. \tag{1.14}$$

Wegen 1.4.2 gilt dann

$$\operatorname{graph}(f) \text{ diophantisch} \iff \operatorname{graph}(f^{-1}) \text{ diophantisch} \,, \tag{1.15}$$

damit folgt dann die Behauptung. □

Mit Hilfe einiger der vorstehenden Lemmatas lassen sich in Ergänzung der anfangs dargestellten diophantischen Relationen weitere angeben.

Lemma 1.4.10 *Sei $c \in \mathbb{N}_0$. Die Relationen $\equiv \pmod c$, $\equiv \pmod{\cdot}$ $\perp$ (teilerfremd zu) und die Funktionen $+$, $-$, $\cdot$, $\operatorname{rem}(\cdot, \cdot)$, $\operatorname{quo}(\cdot, \cdot)$ sind diophantisch.*

Beweis :

<u>„$\equiv \pmod c$“:</u>

Sei $P_1(a_1, a_2, x) := a_1 - a_2 + cx$, $P_2(a_1, a_2, x) := a_1 - a_2 - cx$. Dann gilt zunächst $a_1 \equiv a_2 \pmod c \iff \exists x \in \mathbb{Z} : a_1 - a_2 - cx = 0$. Daraus ergibt sich:

$$a_1 \equiv a_2 \pmod c \iff \left\{ \begin{array}{ll} & \exists x \in \mathbb{N}_0 : P_1(a_1, a_2, x) = 0 \\ \vee & \exists x \in \mathbb{N}_0 : P_2(a_1, a_2, x) = 0 \,. \end{array} \right. \tag{1.16}$$

Beide Zeilen rechts sind jeweils für sich genommen diophantisch; damit ist die ganze Relation rechts wegen Lemma 1.4.3 diophantisch.

„$a_1 \equiv a_2 \pmod{a_3}$“:

Ähnlich wie oben setzen wir $P_1(a_1, a_2, a_3) := a_1 - a_2 + xa_3$, $P_2(a_1, a_2, a_3, x) := a_1 - a_2 - xa_3$.

$$a_1 \equiv a_2 \pmod{a_3} \iff \begin{cases} & \exists x \in \mathbb{N}_0 : P_1(a_1, a_2, a_3, x) = 0 \\ \vee & \exists x \in \mathbb{N}_0 : P_2(a_1, a_2, a_3, x) = 0\,. \end{cases} \tag{1.17}$$

Beide Zeilen rechts sind jeweils für sich genommen diophantisch, damit ist die ganze Relation rechts wegen Lemma 1.4.3 diophantisch.

„$\perp$“:

Es ist $a_1 \perp a_2 \iff \exists x_1, x_2 \in \mathbb{Z} : x_1 a_1 + x_2 a_2 = 1$. Sei zunächst $a_1, a_2 > 0$. Ist dann $x_1 \leq 0$, so muß zur Erfüllung der Gleichung $x_2 > 0$ sein, und ist $x_1 > 0$, so folgt $x_2 \leq 0$. Wenn nun $a_1 = 0$ oder $a_2 = 0$, so ist x_1 bzw. x_2 unbestimmt. Wir können deshalb die Lösung auf den Fall $x_1 x_2 \leq 0$ beschränken und damit schreiben:

$$\begin{aligned} a_1 \perp a_2 &\iff \exists x_1, x_2 \in \mathbb{Z} : \quad x_1 x_2 \leq 0 \quad \wedge \quad x_1 a_1 + x_2 a_2 = 1 \\ &\iff \begin{cases} & \exists x_1, -x_2 \in \mathbb{N}_0 : a_1 x_1 + a_2 x_2 = 1 \\ \vee & \exists -x_1, x_2 \in \mathbb{N}_0 : a_1 x_1 + a_2 x_2 = 1\,. \end{cases} \end{aligned}$$

Wir setzen $P_1(a_1, a_2, x_1, x_2) := x_1 a_1 - x_2 a_2 - 1$, $P_2(a_1, a_2, x_1, x_2) := -x_1 a_1 + x_2 a_2 - 1$.

Damit ergibt sich

$$a_1 \perp a_2 \iff \begin{cases} & \exists x_1, x_2 \in \mathbb{N}_0 : P_1(a_1, a_2, x_1, x_2) = 0 \\ \vee & \exists x_1, x_2 \in \mathbb{N}_0 : P_2(a_1, a_2, x_1, x_2) = 0\,. \end{cases}$$

Beide Zeilen rechts sind jeweils für sich genommen diophantisch, damit ist die ganze Relation rechts wegen Lemma 1.4.3 diophantisch und damit auch die Relation $\perp$.

„$+, -, \cdot$“:

Wir behandeln alle drei Operatoren gleichzeitig. Man ersetze deshalb die folgenden Paare von geschweiften Klammern durch jeweils einen der drei Operatoren. Wir setzen

$$P(a_1, a_2, a_3) := (a_1 \left\{ \begin{array}{c} + \\ - \\ \cdot \end{array} \right\} a_2 - a_3). \tag{1.18}$$

Dann gilt

$$a_1 \left\{ \begin{array}{c} + \\ - \\ \cdot \end{array} \right\} a_2 = a_3 \iff P(a_1, a_2, a_3) = 0\,. \tag{1.19}$$

„rem“:

Für $x, y, z \in \mathbb{N}_0$ ist die Gleichung $z = \mathrm{rem}(y, x)$ äquivalent zu $z \equiv y \pmod{x}$ und $z < x$. Damit können wir schreiben:

$$(y, x, z) \in \mathrm{graph}(\mathrm{rem}) \iff (z \equiv y \pmod{x}) \wedge (z < x)\;. \tag{1.20}$$

Die rechte Seite ist diophantisch und damit auch die Funktion rem.

„quo“:

Die Gleichung $z = \mathrm{quo}(y, x)$ ist äquivalent zu $\exists t \in \mathbb{N}_0 : y = zx + t$ und $t < x$. Damit können wir schreiben:

$$(y, x, z) \in \mathrm{graph}(\mathrm{quo}) \iff \exists t \in \mathbb{N}_0 : (y = zx + t) \wedge (t < x) \ . \tag{1.21}$$

Die rechte Seite ist wieder diophantisch und damit auch die Funktion quo.

□

Kapitel 2

Darstellung der Exponentialfunktion als diophantische Funktion

Einer der wesentlichsten Schritte — im historischen Verlauf der jüngste — zum Beweis der Äquivalenz zwischen Aufzählbarkeit und Diophantizität von Mengen ist der Beweis, daß die Exponentialfunktion x^y diophantisch ist. Bis zum Beweis dieser Tatsache durch [2] wurde der Begriff der exponential–diophantischen Menge verwendet, der sich von unserem Begriff der diophantischen Menge darin unterscheidet, daß die Polynome durch Summen und Produkte von Exponentialfunktionen ersetzt sind oder anders ausgedrückt: Als Exponenten in den Polynomen dürfen auch die in den Relationen auftauchenden Parameter verwendet werden. (Damit sind sie dann im Sinne unserer Definition keine diophantischen Gleichungen mehr). Da dieser Begriff für uns nur bei der historischen Betrachtung eine Rolle spielt, soll er hier nicht eingehender erläutert werden.

Die Äquivalenz des Begriffes der exponential–diophantischen Mengen mit dem der aufzählbaren Mengen wurde von Martin Davis, Hilary Putnam und Julia Robinson [3] 1961 gezeigt. Mit diesem Schritt fehlte nur noch ein Schritt zum Beweis von 1.3.1, nämlich der Beweis, daß die Exponentialfunktion diophantisch ist. Dieses Kapitel soll nun zu diesem Beweis hinführen.

Wie kann man nun zeigen, daß die Exponentialfunktion[1] diophantisch ist? Es liegt nahe, daß das Problem nicht die Abhänigkeit der Funktion x^y von der Basis x, sondern von dem Exponenten y ist, denn bei festgehaltenem Exponenten ist x^y ein Polynom in x und damit diophantisch. Umgekehrt erhalten wir aus der Diophantizität von $x \mapsto a^x$ mit $2 \leq a \in I\!N$ leicht die Diophantizität der Exponentialfunktion (s. Abschnitt 2.4).[2]

Deshalb sucht man nun zunächst eine diophantische Funktion, die sich möglichst ähnlich verhält wie die Exponentialfunktion $x \mapsto a^x$. Leider wird man hier nicht so schnell fündig, und so verringert man seine Ansprüche dahingehend, wenigstens eine diophantische Menge zu finden, deren Elemente ein „ähnliches“ Wachstum haben wie die Potenzen einer bestimmten Zahl.[3]

Tatsächlich liefert so etwas die Pellschen Gleichung

$$a^2 - db^2 = 1 \tag{2.1}$$

[1] Der Abkürzung wegen verstehen wir darunter sowohl eine Funktion $I\!N_0^2 \longrightarrow I\!N_0$ mit $(x, y) \mapsto x^y$ als auch — in üblicher Bedeutung — eine Funktion $I\!N_0 \longrightarrow I\!N_0$ mit $x \mapsto a^x$, wobei $a \in I\!N_0$ ein Parameter ist.

[2] Um aber die Diophantizität der ersteren Funktion nachzuweisen, ist es nötig, die Basis immer als Parameter (i. S. der Definition der Diophantizität) mitzuführen. Für die meisten Betrachtungen wird aber die Exponentialfunktion nur als Funktion des Exponenten mit fester Basis betrachtet. Diese feste Basis wird dann meist ohne Probleme durch einen Parameter ersetzt.

[3] Allerdings darf diese Zahl so bestimmt nicht sein, sie wird später die Rolle eines Parameters i. S. der Diophantizität übernehmen. Zur ersten Orientierung genügt aber diese Formulierung.

als Gleichung in den ganzen Zahlen a und b. Wie gezeigt werden wird, liegen die Lösungen dieser Gleichung „nahe“ den Potenzen einer von d abhängigen nichtrationalen Zahl. Um nun zu einer diophantischen Gleichung für die Exponentialfunktion zu gelangen, benötigt man zwei Schritte:

1. Die Pellsche Gleichung liefert eine Menge von Zahlen, die „nahe“ den Potenzen einer nicht–rationalen Zahl liegen. Daraus haben wir eine diophantische Funktion (von n) zu gewinnen, die die Zahl liefert, die „nahe“ der n-ten Potenz jener nichtrationalen Zahl liegt. Allerdings reicht dafür eine einzige Pellsche Gleichung nicht aus; deshalb wird die die Pellsche Gleichung parametrisierende Variable d zu einem Parameter im Sinne der Definition einer diophantischen Menge.

2. Aus dieser Funktion muß dann die Exponentialfunktion gewonnen werden. Dies ist der leichtere Teil.

Wir werden nun wie folgt vorgehen:

1. Zunächst werden die Eigenschaften der Pellschen Gleichung untersucht (Abschnitt 2.1).

2. Dann wird eine Methode entwickelt, aus der diophantischen Gleichung für die Menge von Potenzen zur diophantischen Gleichung für die Exponentialfunktion selbst zu gelangen, was zwar nicht für den darauf folgenden Abschnitt vorausgesetzt wird, aber die gleiche Problematik in einem etwas einfacheren Fall darstellt (Abschnitt 2.2).

3. Danach wird das Verfahren auf die Lösungen der Pellschen Gleichung übertragen (Abschnitt 2.3). Damit erhält man eine Funktion, die sich „fast“ so verhält wie eine Exponentialfunktion einer nichtrationalen Basis.

4. Schließlich wird aus dieser diophantischen Funktion die Exponentialfunktion selbst gewonnen (Abschnitt 2.4).

5. Zur Ergänzung werden diophantische Gleichungen für einige weitere Funktionen entwickelt, die für den Beweis des zentralen Satzes 1.3.3 benötigt werden (Abschnitt 2.5).

Diese Vorbemerkungen sind in der Ausdrucksweise natürlich unpräzise und sollen nur eine gewisse Vorstellung über die uns erwartenden Aufgaben geben.

2.1 Die Pellsche Gleichung

q

Definition 2.1.1 *Unter einer Pellschen Gleichung verstehen wir eine Gleichung der Art:*

$$a^2 - db^2 = 1\,, \tag{2.2}$$

wobei der Parameter $d \in \mathbb{N}$ kein Quadrat einer ganzen Zahl ist (insbesondere $d \geq 2$) und $(a,b) \in \mathbb{Z}^2$ gesucht sind.

Bemerkung 2.1.2

(i) *Sieht man von der für die Diophantizität unwesentlichen Tatsache ab, daß für a und b auch negative Zahlen zugelassen sind,*[4] *so ist jede Pellsche Gleichung eine von d abhängige diophantische Gleichung in (a, b) (Unbekannte treten keine auf). Die Menge der nichtnegativen Lösungen*[5] $M_d := \{(a, b) \in \mathbb{N}_0^2 \text{ mit } a^2 - db^2 = 1\} \subset \mathbb{N}_0^2$ *ist damit eine diophantische Menge.*

(ii) *Setzt man in (2.2) für d eine quadratische Zahl ein, d. h. $d = c^2$, $c \in \mathbb{N}_0$ (in diesem Fall ist also (2.2) laut Definition keine Pellsche Gleichung mehr), so ergibt sich $(a - cb)(a + cb) = 1$. Damit folgt, daß $a - cb, a + cb = \pm 1$ sind. Daraus folgt $a, cb \in \{-1, 0, 1\}$. Für $c > 1$ existieren daher nur die Lösungen $(\pm 1, 0)$, für $c = 1$ die Lösungen $(\pm 1, 0), (0, \pm 1)$, und für $c = 0$ hat man als Lösungsmenge $\{-1, 1\} \times \mathbb{Z}$. Also passiert in diesem Falle nichts Interessantes, und die Einschränkung auf nichtquadratische d ist berechtigt.*

Wir wollen nun die Struktur der Lösungen von (2.2) bestimmen. Dies wird fast den ganzen übrigen Abschnitt einnehmen.

Lemma 2.1.3 *Die Module $\mathbb{Z}^2$ (mit der komponentenweisen Addition) und $\mathbb{Z}[\sqrt{d}]$ sind isomorph (d nichtquadratisch) mittels der Abbildung*

$$\begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}[\sqrt{d}] \\ (a, b) & \longmapsto & a + b\sqrt{d}\,. \end{array} \tag{2.3}$$

Beweis :

S. Algebra, z. B. [6]. □

Da $\mathbb{Z}[\sqrt{d}]$ ein Ring ist, so induziert die Multiplikation in $\mathbb{Z}[\sqrt{d}]$ eine Multiplikation in $\mathbb{Z}^2$. Wenn wir im weiteren von der Multiplikation auf $\mathbb{Z}^2$ sprechen, so meinen wir immer diese induzierte Multiplikation.

Diese Multiplikation ist besonders interessant im Hinblick auf die Lösungen der Pellschen Gleichung, wie weiter unten gezeigt werden wird.

Definition 2.1.4 *Wir definieren die* **Konjungierte** *zu $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ als $\overline{a + b\sqrt{d}} := a - b\sqrt{d}$. Unter der* **Norm** *von $a + b\sqrt{d}$ verstehen wir $N(a + b\sqrt{d}) := \overline{(a + b\sqrt{d})}(a + b\sqrt{d}) = a^2 - db^2$.*

Lemma 2.1.5 *Die Norm ist multiplikativ, d. h. sie ist ein Halbgruppenhomomorphismus der multiplikativen Halbgruppe von $\mathbb{Z}[\sqrt{d}]$ auf die multiplikative Halbgruppe $\mathbb{Z}$.*

Beweis :

Die Konjugation ist ein Automorphismus auf $\mathbb{Z}[\sqrt{d}]$.[6] Denn für $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ gilt

$$\begin{aligned} \overline{(a + b\sqrt{d}) + (a' + b'\sqrt{d})} &= \overline{(a + a') + (b + b')\sqrt{d}} \\ &= (a + a') - (b + b')\sqrt{d} \\ &= (a - b\sqrt{d}) + (a' - b'\sqrt{d}) \\ &= \overline{a + b\sqrt{d}} + \overline{a' + b'\sqrt{d}} \end{aligned}$$

[4] Der Grund hierfür wird später ersichtlich werden.

[5] Dies ist wie auch im folgenden im Sinne von $a, b \geq 0$ gemeint.

[6] Für den Beweis wird nur die Multiplikativität der Konjugation verwendet.

und

$$\begin{aligned}\overline{(a+b\sqrt{d})(a'+b'\sqrt{d})} &= \overline{(aa'+dbb')+(ab'+a'b)\sqrt{d}}\\ &= (aa'+dbb')-(ab'+a'b)\sqrt{d}\\ &= (a-b\sqrt{d})(a'-b'\sqrt{d})\\ &= \left(\overline{a+b\sqrt{d}}\right)\left(\overline{a'+b'\sqrt{d}}\right).\end{aligned}$$

Zusätzlich ist wegen $\overline{a+b\sqrt{d}} = 0 \Longleftrightarrow a+b\sqrt{d} = 0$ und $\overline{a-b\sqrt{d}} = a+b\sqrt{d}$ die Konjugation auch bijektiv, und damit folgt ingesamt, daß die Konjugation ein Automorphismus ist.

Damit erhalten wir für N:

$$\begin{aligned}N((a+b\sqrt{d})(a'+b'\sqrt{d})) &= (a+b\sqrt{d})(a'+b'\sqrt{d})\overline{(a+b\sqrt{d})(a'+b'\sqrt{d})}\\ &= (a+b\sqrt{d})(a'+b'\sqrt{d})\left(\overline{a+b\sqrt{d}}\right)\left(\overline{a'+b'\sqrt{d}}\right)\\ &= (a+b\sqrt{d})\overline{(a+b\sqrt{d})}(a'+b'\sqrt{d})\overline{(a'+b'\sqrt{d})}\\ &= N(a+b\sqrt{d})N(a'+b'\sqrt{d}).\end{aligned}$$

□

Das Urbild $N^{-1}(G)$ jeder multiplikativen Unterhalbgruppe G von $\mathbb{Z}$, die selbst eine Gruppe ist, ist selbst wieder eine multiplikative Gruppe in $\mathbb{Z}[\sqrt{d}]$. Denn aus $\alpha, \beta \in N^{-1}(G)$ folgt $N(\alpha\beta) = N(\alpha)N(\beta) \in G$; weiter $N(1) = 1 \in G$, also $1 \in \mathbb{N}^{-1}(G)$; aus $\beta \in N-1(G)$ folgt $N(\beta) = \beta\overline{\beta} \in G$; nun ist $G^{-1} = G \subset \mathbb{Z} \subset \mathbb{Z}[\sqrt{d}]$, damit ist $\overline{\beta}N(\beta)^{-1} \in \mathbb{Z}[\sqrt{d}]$ das inverse Element zu β.

Die multiplikativen Gruppen in $\mathbb{Z}$ sind die Einheitengruppe $\{-1, 1\}$ und deren triviale Untergruppe $\{1\}$. Die Urbilder dieser Mengen unter N, nämlich $\{a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ mit $a^2-db^2 = \pm 1\}$ bzw. $\{a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ mit $a^2-db^2 = 1\}$, sind die Einheitengruppe in $\mathbb{Z}[\sqrt{d}]$ bzw. eine ihrer (nicht unbedingt echten) Untergruppen. Denn das Bild einer Einheit ist notwendigerweise auch eine Einheit, damit umfaßt das Urbild der Einheitengruppe in der Bildmenge die Einheitengruppe der Urbildmenge; andererseits sind die Elemente einer Gruppe invertierbar, damit ist jede multiplikative Gruppe Untergruppe der Einheitengruppe; also stimmt die Einheitengruppe von $\mathbb{Z}[\sqrt{d}]$ mit dem Urbild von $\{-1, 1\}$ unter N überein. Weiterhin ist das Urbild einer Untergruppe immer eine Untergruppe des Urbilds der ganzen Gruppe.

Aufgrund des Isomorphismus zwischen $\mathbb{Z}^2$ und $\mathbb{Z}[\sqrt{d}]$ ist aber $\{a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ mit $a^2 - db^2 = 1\}$ mit der Lösungsmenge der Pellschen Gleichung zu identifizieren, die damit eine multiplikative Untergruppe der Einheitengruppe von $\mathbb{Z}^2$ bildet.

Wir wollen nun zunächst die Struktur der Einheitengruppe von $\mathbb{Z}[\sqrt{d}]$ bestimmen. Die Einbettung von $\mathbb{Z}[\sqrt{d}]$ in $\mathbb{R}$ induziert eine Ordnung auf $\mathbb{Z}[\sqrt{d}]$. Mit dieser Ordnung zeigt man folgende Lemmata.

Lemma 2.1.6 *Für eine Einheit* $1 < \alpha := a+b\sqrt{d}$ *in* $\mathbb{Z}[\sqrt{d}]$, *d. h.* $\alpha \in \mathbb{Z}[\sqrt{d}]^{\times}$, *gilt* $a, b > 0$.

Beweis :

Da α eine Einheit ist, folgt $N(\alpha) \in \mathbb{Z}^{\times} = \{-1, 1\}$. Also gilt $N(\alpha) = \alpha\overline{\alpha} = \pm 1$, und damit $\overline{\alpha} = \pm\alpha^{-1}$. Wegen $\alpha > 1$ ist $0 < \alpha^{-1} < 1$, und damit $-1 < \overline{\alpha} < 1$. Damit gilt $2a = \alpha + \overline{\alpha} \geq \alpha - 1 > 0$. Entsprechend gilt $2b = \alpha - \overline{\alpha} \geq \alpha - 1 > 0$. □

Lemma 2.1.7 *Für eine Einheit* $1 < \alpha := a + b\sqrt{d}$ *gilt*

$$\alpha > \sqrt{d}\,. \tag{2.4}$$

Ist sogar $N(\alpha) = 1$*, so gilt* $\alpha > 2\sqrt{d}$*.*

Beweis :

Wegen $\alpha > 1$ gilt wegen Lemma 2.1.6 $a, b \geq 1$, also gilt $\alpha \geq 1 + \sqrt{d} > \sqrt{d}$.
Ist sogar $N(\alpha) = 1$, so ist $0 < \overline{\alpha} < 1$ und damit $\alpha > \alpha - \overline{\alpha} = 2b\sqrt{d} \geq 2\sqrt{d}$. □

Lemma 2.1.8 *Die Einheitengruppe* $\mathbb{Z}[\sqrt{d}]^\times$ *kann dargestellt werden durch*

$$\{\pm\alpha_1^m \textit{ mit } m \in \mathbb{Z}\} \tag{2.5}$$

mit dem erzeugenden Element $\alpha_1 \in \mathbb{Z}[\sqrt{d}]^\times$*, d. h.* $\mathbb{Z}[\sqrt{d}]^\times$ *ist isomorph zu* $\mathbb{Z}^\times \times \mathbb{Z}$*. Die Untergruppe der Einheiten mit* $N(\alpha) = 1$ *ist ebenso isomorph zu* $\mathbb{Z}^\times \times \mathbb{Z}$*.*

Beweis :

Sind $1 < \alpha < \beta$ Einheiten, so auch $\beta/\alpha > 1$, und damit, wie gerade gezeigt, auch $\beta/\alpha \geq \sqrt{d}$. Damit folgt $\beta - \alpha = \alpha(\beta/\alpha - 1) > \beta/\alpha - 1 > \sqrt{d} - 1$. Daher sind die Einheiten, die größer 1 sind, weiter als $\sqrt{d} - 1 > 0$ voneinander entfernt sind und deshalb keinen Häufungspunkt haben können. Insbesondere existiert unter den Einheiten $\alpha > 1$ ein kleinstes Element, welches wir als α_1 bezeichnen.

Alle anderen Einheiten $\alpha > 1$ sind Potenzen dieses Elements, denn sonst würde ein $n \in \mathbb{N}$ existieren mit $\alpha_1^n < \alpha < \alpha_1^{n+1}$. Dann wäre aber $\alpha\alpha_1^{-n}$ eine Einheit mit $1 < \alpha\alpha_1^{-n} < \alpha_1$ im Widerspruch zur Definition von α_1 als kleinstes Element größer 1.

Wenden wir uns nun den Einheiten $0 < \alpha < 1$ zu. Aus $0 < \alpha < 1$ folgt $\alpha^{-1} > 1$, also existiert $n \in \mathbb{N}$ mit $\alpha^{-1} = \alpha_1^n$, d. h. $\alpha = \alpha_1^{-n}$.

Ist α eine Einheit mit $\alpha < 0$, so ist $-\alpha$ eine positive Einheit, also gilt $\alpha = -\alpha_1^m$ mit $m \in \mathbb{Z}$.

Damit ergibt sich die behauptete Struktur von $\mathbb{Z}[\sqrt{d}]^\times$.

Die Einheiten mit $N(\alpha) = 1$ bilden eine Untergruppe vom Index $n = 1$ oder $n = 2$, denn $N(\alpha^2) = N(\alpha)^2 = 1$. Im Fall $n = 1$ ist die Untergruppe mit der Einheitengruppe identisch. Im Fall $n = 2$ ist $N(\alpha_1) = -1$, und die Untergruppe besteht bis auf Vorzeichen aus den geraden Potenzen von α_1, d. h. sie ist identisch mit

$$\{\pm\alpha_1^m \text{ mit } m \in 2\mathbb{Z}\}\,. \tag{2.6}$$

In beiden Fällen ist damit die Untegruppe wieder isomorph zu $\mathbb{Z}^\times \times \mathbb{Z}$. □

Für die Betrachtung der Pellschen Gleichung als diophantische Gleichung muß man sich auf die nichtnegativen Lösungen der Pellschen Gleichung beschränken. Hier erhält man das folgende Resultat, welches das Fundament für den Abschnitt 2.3 liefert.

Lemma 2.1.9 *Für* $a, b \geq 0$ *gilt:*

$$a^2 - db^2 = 1 \iff \exists m \in \mathbb{N}_0 : a + b\sqrt{d} = \alpha_1^m\,, \tag{2.7}$$

dabei ist α_1 *das erzeugende Element aus Lemma 2.1.8.*

Beweis :

$a^2 - db^2 = 1$ ist äquivalent mit $N(a + b\sqrt{d}) = 1$, d. h. $a + b\sqrt{d}$ ist eine Einheit (in $\mathbb{Z}[\sqrt{d}]^\times$).

Aus $a, b \geq 0$ folgt $\alpha := a + b\sqrt{d} > 0$, da 0 selbst keine Einheit ist. Damit folgt $a \geq 1$ oder $b \geq 1$, in jedem Fall folgt $\alpha \geq 1$. Für $\alpha = 1$ ist $\alpha = \alpha_1^0$, und für $\alpha > 1$ ist $\alpha = \alpha_1^m$ mit $m \in \mathbb{N}$.

Umgekehrt ist für jedes α_1^m mit $m \in \mathbb{N}$ wegen Lemma 2.1.6 $a, b > 0$. Für $m = 0$ ist $a, b \geq 0$. Also haben wir genau die behauptete Darstellung. □

Haben wir nun eine Einheit in den Darstellungen als reelle Zahl α und als $a + b\sqrt{d}$, dann fragt sich, ob sich z. B. a aus α direkt berechnen läßt. Die Antwort darauf liefert die folgende Bemerkung.

Bemerkung 2.1.10 *Sei* $1 < \alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ *mit* $N(\alpha) = 1$. *Dann gilt*

$$a = \left\lceil \frac{\alpha}{2} \right\rceil . \tag{2.8}$$

Beweis :

Zunächst gilt wegen Lemma 2.1.6 $a > 0$. Für $a = 1$ folgt $b = 0$, und damit $a = \alpha = 1 = \lceil \frac{1}{2} \rceil$, also gilt die angegebene Gleichung, und wir können im weiteren annehmen, daß $a \geq 2$ ist.

Aus $a^2 - db^2 = 1$ und $b \geq 0$ folgt $b = \frac{a}{\sqrt{d}}\sqrt{1 - \frac{1}{a^2}}$. Also folgt aus $\alpha = a + b\sqrt{d}$ die Gleichung $\alpha = a(1 + \sqrt{1 - \frac{1}{a^2}})$, also

$$a = \frac{\alpha}{1 + \sqrt{1 - \frac{1}{a^2}}} . \tag{2.9}$$

Mit Gleichung (2.9) erhält man für $|a - \alpha/2|$ unter Verwendung von $\sqrt{1 - x} \geq 1 - x$ für $0 \leq x \leq 1$:

$$\begin{aligned}
\left| a - \frac{\alpha}{2} \right| &= \alpha \left| \frac{1}{1 + \sqrt{1 - \frac{1}{a^2}}} - \frac{1}{2} \right| \\
&= \alpha \left| \frac{2 - 1 - \sqrt{1 - \frac{1}{a^2}}}{2 + 2\sqrt{1 - \frac{1}{a^2}}} \right| \\
&= \frac{\alpha}{2} \frac{1 - \sqrt{1 - \frac{1}{a^2}}}{1 + \sqrt{1 - \frac{1}{a^2}}} \\
&< \frac{\alpha}{2} \left(1 - \sqrt{1 - \frac{1}{a^2}} \right) \\
&< \frac{\alpha}{2} \frac{1}{a^2} .
\end{aligned}$$

Aus (2.9) folgt für a auch $a > \frac{\alpha}{2}$ und damit

$$\left| a - \frac{\alpha}{2} \right| < \frac{\alpha}{2} \frac{1}{a^2} < \frac{1}{a} < 1 .$$

Wegen $a > \frac{\alpha}{2}$ folgt dann die Behauptung. □

Zusammen mit Lemma 2.1.9 erhalten wir damit, daß die Pellsche Gleichung als Lösungen eine Reihe von Zahlen liefert, die „nahe" den Potenzen einer reellen Zahl liegen. Dieses Resultat wird jedoch nur zum Beweis einer Abschätzung verwendet, sonst wird immer direkt von dem Resultat aus Lemma 2.1.9 ausgegangen.

Ein weiteres Lemma wird in Abschnitt 2.3 benötigt.

Lemma 2.1.11 *Sei ϕ_m die Restklassenabbildung von $\mathbb{Z}$ nach $\mathbb{Z}_m$. Die Abbildung ψ_m von $\mathbb{Z}[\sqrt{d}]$ nach $\mathbb{Z}_m[\sqrt{\phi_m(d)}]$ (genauer $\mathbb{Z}_m[X]/(X^2 - \phi_m(d))$), die durch*

$$\psi_m(a + b\sqrt{d}) := \phi_m(a) + \phi_m(b)\sqrt{\phi_m(d)} \tag{2.10}$$

definiert ist, ist ein Ringhomomorphismus.

Beweis :

Da ψ komponentenweise abbildet, ist ψ sicherlich ein Gruppenhomomorphismus der additiven Gruppen.

Weiterhin ist

$$\begin{aligned}
\psi_m\left((a + b\sqrt{d})(a' + b'\sqrt{d})\right) &= \psi_m\left(aa' + dbb' + (ab' + a'b)\sqrt{d}\right) \\
&= \phi_m(aa' + dbb') + \phi_m(ab' + a'b)\sqrt{\phi_m(d)} \\
&= \phi_m(a)\phi_m(a') + \phi_m(d)\phi_m(b)\phi_m(b') \\
&\quad + (\phi_m(a)\phi_m(b') + \phi_m(a')\phi_m(b))\sqrt{\phi_m(d)} \\
&= \left(\phi_m(a) + \phi_m(b)\sqrt{\phi_m(d)}\right)\left(\phi_m(a') + \phi_m(b')\sqrt{\phi_m(d)}\right) \\
&= \psi_m(a + b\sqrt{d})\psi_m(a' + b'\sqrt{d}),
\end{aligned}$$

somit ist ψ_m ein Ringhomomorphismus. □

Zur Ergänzung der Thematik noch die folgende Bemerkung:

Bemerkung 2.1.12

(i) *α_1 ist nichtrational. Denn $\alpha_1 = a_1 + b_1\sqrt{d} > 1$, also gilt nach Lemma 2.1.6 $a_1, b_1 \geq 1$. Da nach Voraussetzung d quadratfrei, so ist $\sqrt{d}$ nichtrational und damit auch α_1.*

(ii) *Die Einheiten α mit $N(\alpha) = 1$ bilden eine Untergruppe der Einheitengruppe. Wie schon angedeutet, ist es nicht notwendigerweise eine echte Untergruppe. Ist die betrachtete Untergruppe identisch mit der Einheitengruppe, so heißt dies, daß keine α existieren mit $N(\alpha) = -1$. Tatsächlich tritt dieser Fall bei einigen d auf, bei anderen nicht.*

Bei $d = 3$ ist $N(2 + \sqrt{3}) = 1$. Gäbe es nun ein α mit $N(\alpha) = -1$, so würde mittels den im Beweis von Lemma 2.1.8 angewandten Argumenten die Existenz eines $1 < \alpha' = a' + b'\sqrt{3} < 2 + \sqrt{3}$ mit $N(\alpha') = -1$ folgen. Aus Lemma 2.1.6 ergibt sich $a', b' \geq 1$. Aus $\alpha' < 2 + \sqrt{3}$ folgt damit aber $a', b' \leq 1$. Also folgt $a', b' = 1$, aber $N(1 + \sqrt{3}) \neq -1$. Also gibt es überhaupt keine Einheiten α mit $N(\alpha) = -1$. Tatsächlich ist $d = 3$ ein Spezialfall der Bemerkung 2.3.1.

Bei $d = 5$ ist $N(2 + \sqrt{5}) = 4 - 5 = -1$, also gibt es hier Einheiten mit $N(\alpha) = -1$.

(iii) *Die hier hergeleitete Struktur der Einheitengruppe ist ein Spezialfall des Dirichletschen Einheitensatzes, der allgemein die Strukturen von Einheitengruppen von Zahlkörpererweiterungen behandelt. Dies wird z. B. in [7] dargestellt.*

Zusammenfassend können wir nun sagen, daß wir eine diophantische Menge gewonnen haben, deren Elemente nach oben gerundete Funktionswerte einer Exponentialfunktion ($\mathbb{N} \longrightarrow \mathbb{R}$) mit einer nichtrationalen Basis sind.

Die Aufgabe besteht — wie zu Anfang des Kapitels schon gesagt — nun darin, durch diophantische Gleichungen auch den Exponenten zu bestimmen, oder anders ausgedrückt: Aus dem Bild der Exponentialfunktion muß der Graph der Exponentialfunktion mittels diophantischer Gleichungen bestimmt werden. Wir bezeichnen dies kurz als Abzählung, da quasi die Elemente der Menge durch den Exponenten abgezählt werden. Dies werden wir im nächsten Abschnitt in einer etwas einfacheren Situation durchführen, nämlich für Potenzen natürlicher Zahlen, d. h. wenn die Basis eine natürliche Zahl ist.

2.2 Die Abzählung der Potenzmenge

Mit den Lösungen der Pellschen Gleichung erhalten wir eine Menge von Zahlen, die sich „fast“ so verhalten wie Potenzen einer reellen Zahl. Da wir aber möglichst eine Funktion haben wollen, die sich „fast“ so verhält wie eine Exponentialfunktion, so benötigen wir bei einer Lösung der Pellschen Gleichung zusätzlich auch die Information, welche Potenz des erzeugenden Elements die Lösung darstellt. Wenn es möglich ist, mittels einer diophantischen Relation diese Information zu erhalten, dann haben wir eine diophantische „Fast“–Exponentialfunktion.

Da die Lösungen der Pellschen Gleichung nicht so handlich sind, begeben wir uns auf die Analogie der Potenzen natürlicher Zahlen und betrachten die Relation P: „y ist eine Potenz von x“. Wie wir in diesem Abschnitt zeigen werden, läßt sich hier der Exponent diophantisch bestimmen, d. h. aus einer diophantischen Relation für P läßt sich eine diophantische Gleichung für x^n als Funktion von x, n bestimmen. Dieser Übergang wird dann an die Lösungen der Pellschen Gleichung angepaßt werden, und man erhält damit die oben gesuchte „Fast–Exponentialfunktion“.

Wir werden im folgenden als Parameter y, x, n u. a. verwenden, wobei i. a. y eine Potenz bezeichnet, n den Exponenten und x die Basis. Dies entspricht nicht der Wahl der Parameter bei der Definition von Diophantizität, hat aber den Vorteil, daß man bei mehreren vorkommenden Potenzen eher den Überblick behalten kann.

Definition 2.2.1 *Wir definieren die Relation $P(y,x)$ auf $\mathbb{N}_0^2$ und die Funktion $f : \mathbb{N}_0^2 \to \mathbb{N}$ wie folgt:*

$$\begin{aligned} P(y,x) \quad &:\Longleftrightarrow \quad \exists m \in \mathbb{N}_0 : y = x^m \,, \\ f(x,n) \quad &:= \quad x^n \,. \end{aligned}$$

In diesem Kapitel werden wir den Beweis der folgenden Implikation entwickeln.

Satz 2.2.2

$$P \text{ diophantisch} \Longrightarrow f \text{ diophantisch}\,. \tag{2.11}$$

Wir wollen den Zugang in mehrere Stufen aufteilen. Dabei gehen wir in den Stufen 1–5 von der Generalvoraussetzung

$$x, n, y, k, \ell, m \in \mathbb{N}_0 \text{ und } x \geq 2 \tag{2.12}$$

aus. Weiterhin können wir von $\underline{P \text{ diophantisch}}$ ausgehen, da wir (2.2.2) beweisen wollen.

Zunächst geben wir ein einfaches Lemma an, das wir häufig ohne besondere Erwähnung verwenden.

Lemma 2.2.3 *Für $x, n \in I\!N_0$ und $x \geq 2$ gilt: $n \leq x^n - 1$.*

Beweis :

Es ist $x^n \geq 2^n = (1+1)^n \geq 1 + n$. □

Weiterhin werden wir ohne besondere Erwähnung folgende triviale Beziehungen verwenden: Sei $n, m, \ell \in I\!N_0$. Dann folgt aus $n, m < \ell$ und $n \equiv m \pmod{\ell}$, daß $n = m$. (Denn sei o. E. $n < m$. Ist $n \neq m$, so folgt $m \geq n + \ell \geq \ell$, im Widerspruch zur Voraussetzung.) Weiterhin sind $m \equiv n \pmod{\ell}$ und $\ell | m - n$ äquivalent und aus $m \equiv n \pmod{\ell}$ und $k | \ell$ folgt $m \equiv n \pmod{k}$.

2.2.1 Stufe 1

Die Aufgabe ist es, die Gleichung $y = x^n$ mit Hilfe der Relation P und weiterer diophantischer Relationen auszudrücken. $P(y, x)$ liefert nur: $\exists m \in I\!N$ mit $y = x^m$. Wir benötigen also $n = m$. Die Variable m tritt aber in $P(y, x)$ nicht auf, wir müssen m deshalb durch y, x beschreiben.

Wir schreiben zunächst für $x > 2$

$$x^n = (x - 1 + 1)^n = \sum_{i=0}^{n} \binom{n}{i} (x-1)^i = 1 + n(x-1) + \binom{n}{2} (x-1)^2 + \dots . \tag{2.13}$$

Das ergibt $\mathrm{quo}(x^n, x-1) = n + \binom{n}{2} (x-1) + \dots$, also

$$\mathrm{quo}(x^n, x-1) \equiv n \pmod{x-1} . \tag{2.14}$$

Dieses Ergebnis (nicht die Herleitung) gilt auch für $x = 2$ (denn $a \equiv b \pmod 1 \; \forall a, b \in Z\!\!\!Z$). Damit schreiben wir nun:

$$y = x^n \Longrightarrow \begin{cases} \text{(1a)} & P(y, x) \\ \wedge\text{(1b)} & \mathrm{quo}(y, x-1) \equiv n \pmod{x-1} \\ \wedge\text{(1c)} & n \leq y - 1 . \end{cases} \tag{1}$$

Beweis von (1):

(1a) ist klar. Wegen (2.14) folgt (1b). (1c) folgt aus Lemma 2.2.3. □

Ist P diophantisch, so sind (1a)–(1c) diophantisch und damit die ganze rechte Seite. Wir haben jedoch nur eine Implikation von der linken Seite zur rechten Seite, aber keine Äquivalenz der beiden Seiten.

Die Implikation von rechts nach links scheitert daran, daß aus $P(y, x)$ nur die Existenz eines $m \in I\!N_0$ mit $y = x^m$ folgt; daraus läßt sich mit Hilfe von (2.14) aber nur $m \equiv n \pmod{x-1}$ herleiten. Wir benötigen aber $m = n$.

Da aus $y = x^m$ die Ungleichung $m < y$ folgt und wegen (1c) $n < y$, reicht für $m = n$ zwar zu zeigen, daß $m \equiv n \pmod{z}$ mit $z \geq y$, aber $m \equiv n \pmod{x-1}$ ist ungenügend.

2.2.2 Stufe 2

Um nun eine Kongruenz mit einem genügend großen Modul $z \geq y$ zu erhalten, führen wir ein zweites Zahlenpaar $(\bar{y}, \bar{x})$ ein, wobei $\bar{y}$ dieselbe Potenz von $\bar{x}$ sein soll, wie y von x. Dies drücken wir am kürzesten durch $P(\bar{y}, \bar{x})$ und $\log_{\bar{x}} \bar{y} = \log_x y$ aus, letzteres bezeichnen wir als Relation Q, die wir aber nicht als diophantisch voraussetzen dürfen.

$$Q(y_1, x_1, y_2, x_2) :\Longleftrightarrow \log_{x_1} y_1 = \log_{x_2} y_2 \,. \tag{2.15}$$

Damit das zweite Zahlenpaar Verwendung finden kann, wählen wir $\bar{x}$ genügend groß — hierfür reicht $\bar{x} > y$ —, damit nun die sich aus 2.14 ergebende Kongruenz hinreichend ist.

Mit der Definition von Q und der Ungleichung für $\bar{x}$ können wir schreiben:

$$y = x^n \Longleftrightarrow \exists \bar{y}, \bar{x} \quad \text{mit} \quad \begin{cases} \text{(2a)} & P(y, x) \\ \wedge\text{(2b)} & P(\bar{y}, \bar{x}) \\ \wedge\text{(2c)} & Q(\bar{y}, \bar{x}, y, x) \\ \wedge\text{(2d)} & \operatorname{quo}(\bar{y}, \bar{x} - 1) \equiv n \pmod{\bar{x} - 1} \\ \wedge\text{(2e)} & \bar{x} \geq y + 1 \\ \wedge\text{(2f)} & n \leq y - 1 \,. \end{cases} \tag{2}$$

Beweis :

„$\Rightarrow$“: (2a) ist klar. Wir setzen $\bar{x} := y + 1 \geq 2^0 + 1 = 2$, damit gilt (2e). Weiter definieren wir $\bar{y} := \bar{x}^n$, damit gilt (2b), (2c) und (2d). (2f) folgt wegen Lemma 2.2.3.

„$\Leftarrow$“: Aus (2a) und (2b) folgt: Es existieren k, ℓ mit $y = x^k$ und $\bar{y} = \bar{x}^\ell$. Wegen (2c) folgt dann $k = \ell$. Damit ist $\bar{y} = \bar{x}^k$. Daraus folgt mittels (2.14) die Kongruenz $\operatorname{quo}(\bar{y}, \bar{x} - 1) \equiv k \pmod{\bar{x} - 1}$. Dies liefert zunächst mit (2d) $k \equiv n \pmod{\bar{x} - 1}$ $(*)$. Aus $y = x^k$ ergibt sich mit Lemma 2.2.3 $k \leq y - 1$. Mit (2f) ergibt sich dann $k, n \leq y - 1$ und daraus mit (2e) $k, n < \bar{x} - 1$. Mit $(*)$ ergibt sich dann $k = n$, also $y = x^n$.

□

Man beachte, daß eine gewisse Willkür bei der Definition von Q besteht. Da wir im weiteren immer von $P(y, x)$ und $P(\bar{y}, \bar{x})$ ausgehen werden, ist es unwichtig, wie Q in den anderen Fällen definiert ist. So wäre es möglich, daß Q auch die Relationen $P(y, x)$ und $P(\bar{y}, \bar{x})$ fordert. Letztlich ist dies aber für die eigentliche Rechnung ohne Belang.

Nun haben wir in (2) gegenüber (1) eine Äquivalenz; dafür tritt auf der rechten Seite eine Relation auf, von der wir entweder zeigen müssen, daß sie eine diophantische Relation ist oder durch eine solche ersetzt werden kann.

2.2.3 Stufe 3

Tatsächlich ist in (2) eine schwächere Formulierung von Q ausreichend, die wir als $\overline{Q}$ bezeichnen und durch

$$\overline{Q}(y_1, x_1, y_2, x_2, z) :\Longleftrightarrow \log_{x_1} y_1 \equiv \log_{x_2} y_2 \pmod{z} \,. \tag{2.16}$$

definieren. In den uns interessierenden Fällen ist $k_1 := \log_{x_1} y_1$, $k_2 := \log_{x_2} y_2$ ganzzahlig, und die Relation oben entspricht $k_1 \equiv k_2 \pmod{z}$.

Mit dieser Definition geben wir eine weitere Darstellung der Relation $y = x^n$:

$$y = x^n \Longrightarrow \exists \bar{y}, \bar{x}, z \quad \text{mit} \quad \begin{cases} \text{(3a)} & P(y,x) \\ \wedge\text{(3b)} & P(\bar{y},\bar{x}) \\ \wedge\text{(3c)} & \overline{Q}(\bar{y},\bar{x},y,x,z) \\ \wedge\text{(3d)} & \mathrm{quo}(\bar{y},\bar{x}-1) \equiv n \pmod{\bar{x}-1} \\ \wedge\text{(3e)} & n+1, y \leq z \\ \wedge\text{(3f)} & \bar{x} \equiv 1 \pmod{z},\ \bar{x} \geq 2\,. \end{cases} \tag{3}$$

Die Verwendung von $\overline{Q}$ anstatt von Q ist möglich, da in (2d) sowieso der Exponent nur modulo $\bar{x}-1$ bestimmt wird. In (2c) wird daher Q durch $\overline{Q}$ ersetzt, wobei als Modul in $\overline{Q}$ nicht $\bar{x}-1$, sondern allgemeiner z verwendet wird. Mittels (3f) wird dafür gesorgt, daß aus der Kongruenz modulo $\bar{x}-1$ auch die Kogruenz modulo z folgt.

Wir wollen nun (3) formal beweisen.

Beweis :

„$\Rightarrow$“: Wir setzen $\bar{x} := y+1 \geq 2$, $\bar{y} := \bar{x}^n$ und $z := \bar{x}-1 = y$. (3a), (3b), (3c) und (3f) folgen damit sofort. Bei (3c) hat man sogar die Gleichheit der Exponenten. Aus $\bar{y} = \bar{x}^n$ folgt mittels (2.14) $\mathrm{quo}(\bar{y},\bar{x}-1) \equiv n \pmod{\bar{x}-1}$ und damit (3d). Weiterhin haben wir direkt $y = z$, und mittels Lemma 2.2.3 erhalten wir aus $y = x^n$ die Ungleichung $n \leq y-1 \leq z-1$, und damit folgt (3e).

„$\Leftarrow$“: Aus (3a) und (3b) folgt: Es existieren k, ℓ mit $y = x^k$ und $\bar{y} = \bar{x}^\ell$. Wegen (3c) und (3f) folgt dann $k \equiv \ell \pmod{z}$. Aus $\bar{y} = \bar{x}^\ell$ folgt $\mathrm{quo}(\bar{y},\bar{x}-1) \equiv \ell \pmod{\bar{x}-1}$. Dies liefert mit (3f) und (3d) $\ell \equiv n \pmod{z}$.

Ingesamt ergibt sich $k \equiv n \pmod{z}$ $(*)$. Aus $y = x^k$ ergibt sich $k \leq y-1$ und mit (3e) $k \leq z-1$. Aus (3e) ergibt sich dann weiter $k, n \leq z-1$. Zusammen mit der Kongruenz $(*)$ ergibt sich $k = n$, also $y = x^n$.

□

2.2.4 Stufe 4

Es bleibt nun zu zeigen, daß $\overline{Q}$ diophantisch ist. Da uns die Exponenten nicht zur Verfügung stehen, müssen wir $k \equiv \ell$ mit Hilfe von $x, \bar{x}, y, \bar{y}$ ausdrücken. Zunächst liegt es nahe, als hinreichende Bedingung für eine Kongruenz zwischen k und ℓ eine Kongruenz zwischen y und $\bar{y}$ zu suchen. Da aber y und $\bar{y}$ Potenzen von verschiedener Basis mit verschiedenen Exponenten sind, suchen wir nach Kongruenzen sowohl bei Exponentenwechsel als auch bei Basiswechsel. Eine solche Kongruenz bei letzterem ist die einfache Beziehung:

$$x_2^m \equiv x_1^m \pmod{x_2 - x_1}\,. \tag{2.17}$$

Eine Kongruenzbeziehung bei Exponentenwechsel liefert die folgende recht einsichtige Aussage:

$$x^k \equiv \pm x^m \pmod{x^\ell + 1} \iff k \equiv m \pmod{\ell}\,. \tag{2.18}$$

Der Beweis erfolgt in Lemma 2.2.4. Die ganz ähnliche Äquivalenz

$$x^k \equiv x^m \pmod{x^\ell - 1} \iff k \equiv m \pmod{\ell} \tag{2.19}$$

kann entsprechend bewiesen werden, führt jedoch nicht zum Ziel, was wir hier aber nicht weiter erläutern werden. Jedoch wird diese Beziehung uns an einer anderen Stelle nützlich sein.

Zur Ausnützung von (2.18) bei y und $\bar{y}$ benötigen wir eine weitere Potenz von x; diese sei $\tilde{y} = x^m$, wobei z nun m teilen sollte. Wir drücken das durch die Relation R aus:

$$R(\tilde{y}, x, \ell) :\Longleftrightarrow \exists m > 0 \text{ mit } \tilde{y} = x^m, \ell | m\,. \tag{2.20}$$

Zur Berücksichtigung des Basiswechsels benötigen wir noch $\tilde{y} + 1 | \bar{x} - x$. Fügen wir nun $\bar{x} \equiv x \pmod{x^z + 1}$ bei (3) auf der rechten Seite hinzu (damit haben wir später dafür zu sorgen, daß die Implikation von links nach rechts weiter gültig bleibt), so können wir $\overline{Q}$ zusammen mit einigen weiteren Relationen mittels R und diophantischen Relationen ausdrücken:

$$\exists z : \left\{ \begin{array}{ll} \text{(3a)} & P(y,x) \\ \wedge\text{(3b)} & P(\bar{y},\bar{x}) \\ \wedge\text{(3c)} & \overline{Q}(y,x,\bar{y},\bar{x},z) \\ \wedge(\text{3e}_2) & z \geq y \\ \wedge(\text{4e}_2) & \bar{x} \equiv x \pmod{x^z+1} \end{array} \right\} \Longleftrightarrow \exists \tilde{y}, \bar{z} \left\{ \begin{array}{ll} \text{(4a)} & P(y,x) \\ \wedge\text{(4b)} & P(\bar{y},\bar{x}) \\ \wedge\text{(4c)} & R(\tilde{y},x,\bar{z}) \\ \wedge\text{(4d)} & \bar{y} \equiv \pm y \pmod{\tilde{y}+1} \\ \wedge\text{(4e)} & \bar{x} \equiv x \pmod{\tilde{y}+1} \\ \wedge\text{(4f)} & \bar{z} \geq y\,. \end{array} \right. \tag{4}$$

Beweis :

„⇒“: (4a) und (4b) sind direkt übernommen. (3a) und (3b) ergeben $\exists k, \ell$ mit $y = x^k$ und $\bar{y} = \bar{x}^\ell$. Wir setzen $\bar{z} := z$ und $\tilde{y} := x^{\bar{z}}$. Damit gilt (4c) und (4f), und aus ($4e_2$) folgt (4e). (3c) impliziert $k \equiv \ell \pmod{z}$. Damit ergibt sich mittels (2.18) $x^k \equiv \pm x^\ell \pmod{x^z + 1}$, und mittels (4e) ergibt sich $x^\ell \equiv \bar{x}^\ell \pmod{\tilde{y} + 1}$, also (4d).

„⇐“: (3a) und (3b) sind direkt übernommen. (3a) und (3b) ergeben wieder $\exists k, \ell$ und $y = x^k$, $\bar{y} = \bar{x}^\ell$. Das ergibt $\bar{y} = \bar{x}^\ell \equiv x^\ell \pmod{\bar{x} - x}$, und mit (4e) folgt $\bar{y} \equiv x^\ell \pmod{\tilde{y} + 1}$. Mit (4d) ergibt sich dann $x^\ell \equiv \pm x^k \pmod{\tilde{y} + 1}$. Mittels (4c) folgt insbesondere $\exists m$ mit $\tilde{y} = x^m$ und $m \geq \bar{z} \geq y$ (letzteres wegen (4f)). Wir setzen $z := m$, dann gilt ($3e_2$), und mit (4e) ergibt sich ($4e_2$). Man erhält weiter $x^\ell \equiv \pm x^k \pmod{x^m + 1}$, und mit (2.18) (Implikation von links nach rechts) folgt $\ell \equiv k \pmod{m}$. Wegen $m = z$ ergibt sich dann (3c).

□

2.2.5 Stufe 5

Bleibt noch R als diophantische Relation auszudrücken. Nun hängt zwar R mit $\overline{Q}$ mittels $R(\tilde{y}, x, \ell) \Longleftrightarrow \overline{Q}(\tilde{y}, x, 2^0, 2, \ell)$ zusammen, aber dieser Spezialfall von $\overline{Q}$ ist leichter diophantisch darzustellen.

Aus (2.14) ergibt sich für $x' \geq 2$:

$$\operatorname{quo}(x'^n, x' - 1) \equiv 0 \pmod{x' - 1} \iff x' - 1 | n\,. \tag{2.21}$$

Setzt man nun $x' := x^k$ ein, so ergibt sich die Äquivalenz

$$\operatorname{quo}((x^k)^n, x^k - 1) \equiv 0 \pmod{x^k - 1} \Longleftrightarrow x^k - 1 | n\,. \tag{2.22}$$

Da wir gerne $z | n$ ausdrücken würden, liegt es nahe, z selbst in der Form $z = x^\ell - 1$ zu wählen.

Um (2.22) anzuwenden, müssen wir dafür sorgen, daß $\tilde{y} = x^m$ eine Potenz von $x^\ell = z+1$ ist, d. h. $\ell | m (*)$. Dies ist aber recht einfach. Wir setzen in (2.19) einfach $m = 0$; das liefert die Äquivalenz

$$x^\ell - 1 | x^k - 1 \iff \ell | k \, . \tag{2.23}$$

Damit können wir die Forderung $(*)$: $\ell | m$ durch $z | \tilde{y} - 1$ ersetzen.
Ingesamt liefert dies also:

$$R(\tilde{y}, x, z) \Longleftarrow \begin{cases} & P(\tilde{y}, x) \\ \wedge & P(z+1, x) \\ \wedge & z | \tilde{y} - 1 \\ \wedge & \operatorname{quo}(\tilde{y}, z) \equiv 0 \pmod{z} \, . \end{cases}$$

Nun noch eine Schönheitskorrektur. Es gilt nämlich entsprechend dem Beweis für (2.14) $\operatorname{quo}(x^m, x^\ell - 1) = (x^m - 1)/(x^\ell - 1)$. Wegen $z =: x^\ell - 1 | \tilde{y} - 1 =: x^m - 1$ ist $\operatorname{quo}(\tilde{y}, z) \equiv 0 \pmod{z}$ äquivalent zu $z | (\tilde{y} - 1)/z$ oder anders geschrieben $z^2 | \tilde{y} - 1$. Damit können wir kürzer schreiben:

$$R(\tilde{y}, x, z) \Longleftarrow \begin{cases} \text{(5a)} & P(\tilde{y}, x) \\ \wedge\text{(5b)} & P(z+1, x) \\ \wedge\text{(5c)} & z^2 | \tilde{y} - 1 \, . \end{cases} \tag{5}$$

Noch einmal der Beweis in kompakter Form:

Beweis :

Aus (5a) und (5b) ergibt sich $\exists m, \ell$ mit $\tilde{y} = x^m$ und $z = x^\ell - 1$. Aus (5c) ergibt sich zunächst $z | \tilde{y} - 1$ und daraus mittels (2.23) die Existenz von i mit $m = i\ell$ und $\tilde{y} = (z+1)^i$. Damit ergibt sich entsprechend dem Beweis für (2.14) (s. o.) $\operatorname{quo}(\tilde{y}, z) = (\tilde{y} - 1)/z$ und wegen (5c) $\operatorname{quo}(\tilde{y}, z) \equiv 0 \pmod{z}$. Andererseits ist $\operatorname{quo}(\tilde{y}, z) = \operatorname{quo}((z+1)^i, z) \equiv i \pmod{z}$. Ingesamt folgt $z | i$ und daraus $z | m$, was zu zeigen war. □

Wir haben nun $R(\tilde{y}, x, z)$ durch hinreichende Bedingungen ausgedrückt. Wenn man nun (5) in (4) und dieses wiederum in die um ($4e_2$) ergänzte rechte Seite von (3) einsetzt, so muß man noch nachweisen, daß man nicht nur eine Implikation sondern sogar eine Äquivalenz erhält.

Man sieht, daß dabei die beiden Forderungen

$$\begin{aligned} \bar{x} &\equiv 1 \pmod{z} \, , \\ \bar{x} &\equiv x \pmod{\tilde{y} + 1} \end{aligned}$$

an $\bar{x}$ die einzige Schwierigkeit bilden.

Damit ein solches $\bar{x}$ existiert, würde die Teilerfremdheit von z und $\tilde{y} + 1$ genügen. Wählt man nun für z einfach $y - 1$, so erhält man wegen der zur Erfüllung von $R(\tilde{y}, x, z)$ notwendigen Bedingung $y - 1 | \tilde{y} - 1$. Wegen $\tilde{y} + 1 \equiv 2 \pmod{y - 1}$ ist der größte gemeinsame Teiler von $\tilde{y} + 1$ und $y - 1$ ein Teiler von 2. Wenn der größte gemeinsame Teiler tatsächlich 2 ist, muß erst noch die Erfüllbarkeit der beiden Kongruenzen für $\bar{x}$ gezeigt werden. In diesem Fall sind aber sicherlich $\tilde{y} + 1$ und $y - 1$ gerade, also x ungerade, also $x - 1$ gerade; damit sind die Kongruenzen auch in diesem Fall erfüllbar. (Wir werden sogar weiter unten $\bar{x}$ direkt angeben.)

Durch die Setzung von z als $y - 1$ haben wir eine weitere Schwierigkeit erkauft. In (3) wird gefordert, daß $y \le z$, was nun nicht mehr erfüllt ist. Dies können wir dadurch ausgleichen, daß wir den Fall $n = 0$ in der Äquivalenz auslassen und ihn explizit behandeln.

Wenn wir nun das alles durchführen, können wir die Diophantizität von f erhalten.

2.2.6 Der vollständige Beweis

Zu Beginn geben wir die in den vorigen Abschnitten entwickelten Beziehungen in einem Lemma an, wobei die Beweise teilweise nicht übernommen sind, sondern direkter geführt werden.

Lemma 2.2.4 *Sei $x, y, n, k, m \in \mathbb{N}_0$. Es gelten die folgenden fünf Aussagen:*

(i) Für $x \geq 2$ gilt: $\mathrm{quo}(x^n, x-1) \equiv n \pmod{x-1}$.

(ii) $x^n \equiv y^n \pmod{y-x}$.

(iii) Für $x \geq 2$ gilt: $x^n - 1 | x^m - 1 \Longleftrightarrow n | m$.

(iv) Für $x \geq 2$ gilt: $(x^n-1)^2 | x^m - 1 \Longleftrightarrow n(x^n-1) | m$.

(v) Für $x \geq 2, k \geq 1$ gilt: $x^n \equiv \pm x^m \pmod{x^k+1} \Longleftrightarrow n \equiv m \pmod{k}$.

Beweis :

(i) Für $x = 2$ ist die Aussage trivial. Wir nehmen also an, daß $x \geq 3$. Dann gilt

$$x^n = (x-1+1)^n = 1 + \sum_{i=1}^{n} \binom{n}{i} (x-1)^i \,. \tag{2.24}$$

Die Summe ist wegen $i \geq 1$ durch $x-1$ teilbar. Wegen $x - 1 > 1$ gilt dann

$$\begin{aligned} \mathrm{quo}(x^n, x-1) &= \sum_{i=1}^{n} \binom{n}{i} (x-1)^{i-1} \\ &= n + \sum_{i=2}^{n} \binom{n}{i} (x-1)^{i-1} \\ &\equiv n \pmod{x-1} \,. \end{aligned}$$

(ii) Es gilt $x^n - y^n = (x-y)\sum_{i=0}^{n-1} x^{n-1-i}y^i$. Daraus folgt die angegebene Kongruenz.[7]

(iii) „$\Leftarrow$“: Für $m = 0$ gilt die linkes Seite direkt. Aus $n|m$ und $m \geq 1$ folgt, daß $\exists \ell \geq 1$ mit $m = \ell n$. Dann folgt

$$x^m - 1 = (x^n)^\ell - 1 = (x^n - 1)\sum_{i=0}^{\ell-1} x^{ni} \,, \tag{2.25}$$

also gilt die linkes Seite von (iii).

(iii) „$\Rightarrow$“: Für $n = 0$ ist die rechte Seite immer erfüllt. Sei also $n \geq 1$, dann existieren $\ell, m' \in \mathbb{N}_0$ und $m' < n$, so daß $m = \ell n + m'$. Damit gilt

$$x^m - 1 = x^{m'}(x^{\ell n} - 1) + x^{m'} - 1 \,. \tag{2.26}$$

Aufgrund von dem schon gezeigten (iii)„$\Leftarrow$“ folgt $(x^n - 1)|(x^{\ell n} - 1)$. Nach Voraussetzung gilt $(x^n-1)|(x^m-1)$, und damit ergibt sich $(x^n-1)|(x^{m'}-1)$. Andererseits ist wegen $m' < n$ und $x \geq 2$ auch $x^{m'} - 1 < x^n - 1$; damit folgt aufgrund der Teilbarkeitsbeziehung: $x^{m'} - 1 = 0$ und daraus $m' = 0$. Das ergibt $m = \ell n$, also $m|n$.

[7] Diese Kongruenz ist zwar ziemlich trivial, da aber die analoge Aussage im nächsten Abschnitt nicht mehr ganz so trivial ist, führen wir ihr Pendant in diesem Abschnitt auf.

(iv) „$\Rightarrow$“: Wie in (iii) können wir ohne Einschränkung annehmen, daß $m \neq 0$. Aus der linken Seite folgt, daß $(x^n-1)|(x^m-1)$. Mit (iii) folgt $n|m$, also $\exists \ell$ mit $m = \ell n$. Damit gilt

$$x^m - 1 = x^{n\ell} - 1 = (x^n - 1)\sum_{i=0}^{\ell-1} x^{in} . \tag{2.27}$$

Nach Voraussetzung folgt dann $(x^n-1)|\sum_{i=0}^{\ell-1} x^{in}$. Also

$$0 \equiv \sum_{i=0}^{\ell-1} x^{in} \equiv \sum_{i=0}^{\ell-1} 1 \equiv \ell \pmod{x^n - 1} . \tag{2.28}$$

Also folgt $x^n - 1|\ell$, und nach Definition von ℓ folgt dann $n(x^n-1)|m$.

(iv) „$\Leftarrow$“: Wir können wieder ohne Einschränkung annehmen, daß $m \neq 0$; damit ist auch $n \neq 0$. Aus $n(x^n-1)|m$ folgt $\exists \ell$ mit $m = \ell n(x^n - 1)$. Damit folgt:

$$x^m - 1 = (x^{n\ell})^{x^n-1} - 1 = (x^{n\ell} - 1)\sum_{i=0}^{x^n-2} (x^{n\ell})^i . \tag{2.29}$$

Weiter ist

$$\sum_{i=0}^{x^n-2} x^{n\ell i} \equiv \sum_{i=0}^{x^n-2} 1 \equiv x^n - 1 \equiv 0 \pmod{x^n - 1} . \tag{2.30}$$

Damit gilt $x^n - 1|\sum_{i=0}^{x^n-2} x^{in\ell}$, außerdem wegen Lemma 2.2.4(iii) $x^n - 1|x^{n\ell} - 1$, also $(x^n-1)^2|(x^m-1)$.

(v) „$\Rightarrow$“: Wegen $k \geq 1$ existieren ℓ_1, n', ℓ_2, m' mit $n = \ell_1 k + n', m = \ell_2 k + m'$ und $0 \leq n', m' \leq k-1$. Dann folgt

$$x^n = x^{n'} x^{\ell_1 k} \equiv x^{n'}(-1)^{\ell_1} \equiv \pm x^{n'} \pmod{x^k + 1} . \tag{2.31}$$

Entsprechend gilt $x^m \equiv \pm x^{m'} \pmod{x^k+1}$. Somit folgt $x^{m'} \equiv \pm x^{n'} \pmod{x^k+1}$. Daraus erhalten wir $(x^k+1)|(x^{m'} \pm x^{n'})$. Ohne Einschränkung können wir $n' > m'$ annehmen, dann folgt $(x^k+1)|(x^{m'}(x^{n'-m'} \pm 1))$. Nun ist, wie man sich leicht überlegt, $x^{m'}$ prim zu x^k+1. Damit gilt $(x^k+1)|(x^{n'-m'} \pm 1)(*)$. Wegen $n' - m' < k$, $k \geq 1$ und $x \geq 2$ folgt $0 \leq x^{n'-m'} \pm 1 < x^k + 1$. Mit $(*)$ folgt dann $x^{n'-m'} \pm 1 = 0$. Mit $x \geq 2$ folgt dann $n' = m'$ und damit $n \equiv m \pmod k$.

(v) „$\Leftarrow$“: Ohne Einschränkung können wir $n \geq m$ annehmen. Dann folgt aus $n \equiv m \pmod k$, daß ein $\ell \in \mathbb{N}$ existiert mit $n = \ell k + m$. Dann gilt

$$x^n = x^m x^{k\ell} \equiv x^m(-1)^\ell \equiv \pm x^m \pmod{x^k + 1} . \tag{2.32}$$

□

Betrachtet man (ii) und (iii), so könnte man meinen, die beiden Aussagen wären Spezialfälle der allgemeineren Aussage, die man aus (iii) durch Ersetzen von 2 durch k erhält, Dies gilt aber nicht. Beispiel: $x = 3$, $n = 3$, $k = 3$, $m = n(x^n-1)^{k-1}/2 = 1014$. Damit würde folgen $n(x^n-1)^{k-1} \not| m$, aber $(x^n-1)^3 = 17576|3^{1014} - 1$. Mit Lemma 2.2.4 sind wir in der Lage, den folgenden Satz zu beweisen:

Satz 2.2.5 *Sei $x, n \in \mathbb{N}_0$ mit $x \geq 2, n \geq 1$. Dann gilt folgende Äquivalenz:*

$$y = x^n \iff \exists \bar{x}, \bar{y}, \tilde{y} \in \mathbb{N}_0 \text{ mit } \begin{cases} (6a) & P(y,x) \\ \wedge(6b) & P(\bar{y},\bar{x}) \\ \wedge(6c) & P(\tilde{y},x) \\ \wedge(6d) & (y-1)^2 | (\tilde{y}-1) \\ \wedge(6e) & \bar{x} \equiv 1 \pmod{y-1} \\ \wedge(6f) & \bar{x} \equiv x \pmod{\tilde{y}+1} \\ \wedge(6g) & \bar{y} \equiv y \pmod{\tilde{y}+1} \\ \wedge(6h) & \operatorname{quo}(\bar{y}, \bar{x}-1) \equiv n \pmod{y-1} \\ \wedge(6i) & n \leq y-1 \\ \wedge(6j) & \tilde{y} \geq y\,. \end{cases} \tag{6}$$

Beweis :

„$\Rightarrow$“: Aussage (6a) ist klar. (6i) folgt aus Lemma 2.2.3. Wir setzen nun $\tilde{y} = x^{n(y-1)}$. Damit folgt (6c), und mit (6i) folgt $y - 1 \geq n \geq 1$ und damit (6j). Aus Lemma 2.2.4(iii) folgt dann $(y-1)^2 | (\tilde{y}-1)$, also (6d). Wir setzen

$$\bar{x} := \begin{cases} x + (\tilde{y}+1)\frac{y}{2}((\tilde{y}+1)(y-1)+1-x) & \text{für } x \text{ gerade} \\ x + (\tilde{y}+1)y((\tilde{y}+1)(y-1)+\frac{1-x}{2}) & \text{für } x \text{ ungerade}\,. \end{cases} \tag{2.33}$$

Nun ist $\bar{x} \in \mathbb{Z}$, da mit x gerade auch y gerade und ist wegen $n \geq 1$ auch $y, \tilde{y} \geq x$ und damit auch $y, \tilde{y} \geq 2$. Damit ist sicherlich $((\tilde{y}+1)(y-1)+1-x) \geq 0$ bzw. $(\tilde{y}+1)(y-1)+\frac{1-x}{2} \geq 0$ und damit $\bar{x} \geq x \geq 2$. erfüllt. Wegen (6d) ergibt sich $\tilde{y}+1 = \tilde{y}-1+2 \equiv 2 \pmod{y-1}$. Damit erhalten wir zusammen mit der Definition von $\bar{x}$ (6e).

Nun setzen wir $\bar{y} = \bar{x}^n$, damit folgt (6b). Mittels Lemma 2.2.4(i) und, wie oben gezeigt, $\bar{x} \geq 2$ und der schon gezeigten (6e) folgt (6h). Wegen (6f) gilt $\tilde{y}+1 | \bar{x}-x$, damit folgt mit Lemma 2.2.4(ii) die Aussage (6g). Damit sind alle Aussagen auf der rechten Seite bewiesen.

„$\Leftarrow$“: Aus der Definition von P ergibt sich aus (6a)–(6c): Es existieren $p, q, r \in \mathbb{N}_0$ mit $y = x^p, \bar{y} = \bar{x}^q, \tilde{y} = x^r$. Also müssen wir zeigen, daß $p = n$. Aus $y = x^p$ ergibt sich $p \leq y-1$, aus (6i) haben wir $n \leq y-1$. Nach Voraussetzung ist $n \geq 1$, damit reicht zu zeigen, daß $n \equiv p \pmod{y-1}$.

(A): Wegen (6j) und $n \geq 1$ ergibt sich $\tilde{y} \geq y \geq x$, damit wegen (6f) $\bar{x} \geq x \geq 2$. Dann ergibt sich nach Lemma 2.2.4(i), daß $\operatorname{quo}(\bar{y}, \bar{x}-1) \equiv q \pmod{\bar{x}-1}$. Wegen (6e) folgt dann $\operatorname{quo}(\bar{y}, \bar{x}-1) \equiv q \pmod{y-1}$. Damit gilt mit (6h), daß $q \equiv n \pmod{y-1}$.

(B): Wegen (6g) haben wir $\bar{x}^q \equiv x^p \pmod{\tilde{y}+1}$. Wegen Lemma 2.2.4(ii) ergibt sich $\bar{x}^q \equiv x^q \pmod{\bar{x}-x}$, mit (6f) folgt dann $\bar{x}^q \equiv x^q \pmod{\tilde{y}+1}$, also ingesamt $x^q \equiv x^p \pmod{x^r+1}$. Nun ist wegen (6j) $\tilde{y} \geq y$, d.h. $r \geq n \geq 1$. Dann folgt mit Lemma 2.2.4(iv) einfach $q \equiv p \pmod{r}$. Aus (6d) ergibt sich aber mittels Lemma 2.2.4(ii), daß $y-1 | r$, damit $q \equiv p \pmod{y-1}$.

(A) und (B) zusammen ergeben die zu zeigende Aussage $n \equiv p \pmod{y-1}$.

□

Wir geben hier weiterhin eine Motivation des Beweises, der die Stufen 1–5, die zu dem Beweis hinführten, zusammenfaßt.

Erläuterung des Beweises: Wir gehen also von $x, y, n \in I\!N_0$ aus. Wie können wir (in diophantischen Relationen) ausdrücken, daß $y = x^n$? Zunächst liegt es nahe, als erste Relation $P(y, x)$ zu verwenden. Die einzige Information, die wir über n haben, ist $n \leq y - 1$. Das liefert uns eine zweite Relation. Aus der ersten ergibt sich aber nur $\exists p$ mit $y = x^p$. Wir müssen also nun das n mit p in Verbindung bringen. Hier liefert uns Lemma 2.2.4(i) einen Ansatz: $\mathrm{quo}(y, x-1) \equiv n \pmod{x-1}$ ergibt $p \equiv n \pmod{x-1}$. Die Schwierigkeit ist, daß n nur durch y begrenzt ist, aber $n \gg x - 1$ ohne weiteres möglich ist. Der Modul ist zu klein, andererseits wäre $y - 1$ als Modul ausreichend.

Deshalb versucht man die p–te Potenz einer hinreichend großen Zahl $\bar{x}$ zu erzeugen und dann Lemma 2.2.4(i) zu verwenden. Das ergibt $P(\bar{y}, \bar{x})$, d. h. Relation (6b) und $\mathrm{quo}(\bar{y}, \bar{x} - 1) \equiv n \pmod{\bar{x} - 1}$. Zunächst liefert dies aber nur $\bar{y} = \bar{x}^q$ und $q \equiv n \pmod{\bar{x} - 1}$.

Statt *einer* Aufgabe ergeben sich jetzt *zwei* Aufgaben, die aber leichter zu lösen sind. Erstens ist p mit q in ausreichender Weise zu verbinden, zweitens ist dafür zu sorgen, daß $\bar{x} - 1 \geq y - 1$, wofür $y - 1 | \bar{x} - 1$ und $\bar{x} > 1$ sicherlich ausreicht, wobei ersteres äquivalent zu (6e) ist.

Wenden wir uns der ersten Aufgabe zu. Wir haben die Potenzen $y = x^p$ und $\bar{y} = \bar{x}^q$. Lemma 2.2.4(iv) liefert aber nur eine Verbindung der Exponenten bei gleicher Basis. Nach Lemma 2.2.4(ii) $\bar{x}^q \equiv x^q \pmod{\bar{x} - x}$. Zur Anwendung des Lemmas 2.2.4(v) müssen wir eine weitere Potenz von x einführen durch $P(\tilde{y}, x)$, d. h. (6c); dies ergibt $\exists r$ mit $\tilde{y} = x^r$. Um das Problem ungleicher Potenzen zu lösen, benötigen wir noch $\tilde{y} + 1 | \bar{x} - x$, was äquivalent zu (6f) ist. Denn nun liefert uns $\bar{y} \equiv y \pmod{\tilde{y} + 1}$ zunächst $x^q \equiv x^p \pmod{x^q + 1}$ und mittels Lemma 2.2.4(v) $q \equiv p \pmod{q}$. Nötig ist zumindest wieder $r \geq y - 1$, wofür wieder $y - 1 | r$ ausreicht.

Hier sollte man sich klar machen, wie nun die Zahlen aussehen: $\tilde{y}$ ist eine r–te Potenz von x; r wiederum ein Vielfaches einer p–ten Potenz von x, d. h. $\tilde{y} = x^{\ell(x^p - 1)}$. Wichtig ist es nun, die Zahl $\tilde{y}$ tatsächlich zu finden, und hier wirkt das wesentlichste Lemma in diesem Beweis, nämlich Lemma 2.2.4(iii). Mit Hilfe von $(y-1)^2 | (y_1 - 1)$ erhalten wir $r | (y - 1)$. Mittels (6j) wird der Trivialfall $r = 0$ ausgeschlossen.

Damit müssen wir nur noch zeigen, daß die Bedingungen auch erfüllbar sind. Hier zeigt es sich, daß höchstens (6e) und (6f) Probleme bereiten. Eine andere Form des Lemmas 2.2.4(v) liefert als Moduln $y - 1, \tilde{y} - 1$ statt $y - 1, \tilde{y} + 1$, wegen (6d) wären dann (6e) und (6f) i. a. nicht zu erfüllen. Deshalb wurde diese Form des Lemmas gewählt. Hier zeigt es sich, daß $y - 1$ und $\tilde{y} + 1$ wegen (6d) nur den gemeinsamen Faktor 2 haben können. Dann ist y und damit x ungerade, und (6e) und (6f) sind gleichzeitig erfüllbar.

Beweis von Satz 2.2.2:

Nun sind wir in der Lage, den Satz 2.2.2 zu beweisen. Unter der Voraussetzung, daß P diophantisch ist, stehen auf der rechten Seite von (6) nur diophantische Relationen. Einzige Schwierigkeit scheint zu sein, daß Satz 2.2.5 nur für $x \geq 2, n \geq 1$ gilt. Dies macht aber dennoch keine Probleme, denn wir schreiben einfach:

$$y = x^n \iff \exists \bar{x}, \bar{y}, \tilde{y} \in I\!N_0 \text{ mit } \left\{ \begin{array}{ll} & (n = 0 \land y = 1) \\ \lor & (n \geq 1 \land x = 0 \land y = 0) \\ \lor & (n \geq 1 \land x = 1 \land y = 1) \\ \lor & (n \geq 1 \land x \geq 2 \land (6a) \land \ldots \land (6j)) \, . \end{array} \right. \tag{2.34}$$

Aufgrund von Lemma 1.4.3 ist die rechte Seite diophantisch und damit auch die linke Seite, dort steht aber $\mathrm{graph}(f)$ als Relation ausgedrückt. Damit ist f diophantisch. □

2.3 Die Abzählung der Lösungen der Pellschen Gleichung

Im vorigen Abschnitt haben wir die Implikation P diophantisch $\Longrightarrow f$ diophantisch bewiesen. Allerdings steht uns keine diophantische Gleichung für P zu Verfügung, so daß die Implikation quasi „in der Luft“ steht.

Tatsächlich wird der vorige Abschnitt uns nur dafür dienen, Anhaltspunkte für unser Vorgehen in diesem Abschnitt zu liefern. Hier gehen wir nun von den Lösungen der Pellschen Gleichung aus, die näherungsweise Potenzen einer nichtrationalen Zahl sind, und suchen nach einer Abzählung dieser Lösungen, was dem Finden einer diophantischen Gleichung für die Exponentialfunktion im vorigen Abschnitt entspricht.

Bei den Bemerkungen zu den Lösungen der Pellschen Gleichung gingen wir von einem $2 \leq d \in \mathbb{N}$ aus — mit der einzigen Einschränkung, daß d kein Quadrat einer natürlichen Zahl sei.

Im allgemeinen ist es recht schwierig, das erzeugende Element zu finden; deshalb liegt es nahe, eine weitere Einschränkung zu machen, nämlich

$$d := x^2 - 1 \text{ mit } 2 \leq x \in \mathbb{N}$$

zu setzen. Letzeres sei für den ganzen Abschnitt vorausgesetzt. Damit liegt $\sqrt{d}$ (für große x) nahe einer natürlichen Zahl.

Es folgt auch, daß ein so gewähltes d für $x \geq 2$ keine Quadratzahl ist: Denn sei $d = c^2 = x^2-1$ mit $c \in \mathbb{N}$, so folgt $(x-c)(x+c) = 1$. Wegen $c, x \in \mathbb{N}$ folgt $x+c, x-c = 1$ und daraus $x = 1$, entgegen der Voraussetzung, daß $x \geq 2$. Neben $d = x^2+1$, das entsprechend auch keine Quadratzahl ist, ist damit $d = x^2 - 1$ die beste Approximation an x^2 durch nichtquadratische ganze Zahlen.

Sei nun $1 < \alpha'_1 = a + b\sqrt{x^2-1} \in \mathbb{Z}[\sqrt{x^2-1}] \subset \mathbb{R}$ das erzeugende Element der Lösungen der Pellschen Gleichung. Nach Lemma 2.1.7 gilt $\alpha'_1 > 2\sqrt{x^2-1}$. Damit folgt aus Bemerkung 2.1.10

$$a > \frac{\alpha'_1}{2} > \sqrt{x^2-1} > x-1\,. \tag{2.35}$$

Also ist $a \geq x$. Aus der Pellschen Gleichung erhält man damit sofort $|b| \geq 1$. Wegen Lemma 2.1.6 folgt $b \geq 1$. Nun genügt aber $a = x$, $b = 1$ der Pellschen Gleichung. Damit ergibt sich als gesuchtes erzeugendes Element (das jeweils das kleinste Element $\alpha > 1$ mit $N(\alpha) = 1$ ist)

$$\alpha'_1 = x + \sqrt{x^2-1}\,.$$

Bemerkung 2.3.1 *Für d in der Form $x^2 - 1$ stimmt die Einheitengruppe von $\mathbb{Z}[\sqrt{d}]$ mit der Lösungsmenge der Pellschen Gleichung überein.*

Beweis :

Sei $\alpha \in \mathbb{Z}[\sqrt{x^2-1}]$ mit $N(\alpha) = -1$. Dann existiert entsprechend dem Beweis von Lemma 2.1.8 ein $\alpha' \in \mathbb{Z}[\sqrt{x^2-1}]$ mit $N(\alpha') = -1$ und $1 < \alpha' < \alpha'_1$. Dann folgt aber $1 < {\alpha'}^2 < {\alpha'_1}^2$ und $N(\alpha^2) = 1$. Damit folgt nun ${\alpha'}^2 = \alpha'_1$. Ist nun aber $\alpha' = a + b\sqrt{x^2-1}$ mit $a, b \in \mathbb{N}_0$, so folgt aus ${\alpha'}^2 = x + \sqrt{x^2-1}$ für a, b: $2ab = 1$. Dies kann aber nicht erfüllt werden, also gibt es kein α mit $N(\alpha) = -1$.

Also ist das erzeugende Element der Einheitengruppe gleichzeitig auch eine Lösung der Pellschen Gleichung. □

Man bemerke, daß das erzeugende Element $x + \sqrt{x^2 - 1}$ nächst der Zahl $2x$ liegt, oder genauer $2x - 1 < x + \sqrt{x^2 - 1} < 2x$. Für eine Lösung $(a, b) \in I\!N^2$ der Pellschen Gleichung gilt $a + b\sqrt{x^2 - 1} = \alpha^n$ und damit $(2x - 1)^n < a + b\sqrt{x^2 - 1} < (2x)^n$ und mit der Gleichung 2.1.10

$$(2x - 1)^n/2 < a < (2x)^n/2 + 1 . \tag{2.36}$$

Als ersten Schritt führen wir zunächst das Analogon zu P und der Exponentialfunktion ein. Da die Pellsche Gleichung Zahlenpaare als Lösungen hat, benötigen wir zwei Relationen und zwei Funktionen. Zur Verstärkung der Analogien bezeichnen wir nun die entsprechenden Lösungen nicht mehr mit (a, b) sondern mit (y_1, y_2) entsprechend unserem $y = x^n$ aus dem vorigen Abschnitt.

Definition 2.3.2 *Wir definieren die Relationen $P_1, P_2 \subset I\!N_0^2$ durch*

$$P_1(y_1, x) \quad :\Longleftrightarrow \quad \exists y_2 \in I\!N_0 : y_1^2 - (x^2 - 1)y_2^2 = 1 , \tag{2.37}$$

$$P_2(y_2, x) \quad :\Longleftrightarrow \quad \exists y_1 \in I\!N_0 : y_1^2 - (x^2 - 1)y_2^2 = 1 , \tag{2.38}$$

wobei für $x = 0, 1$ rechts keine Pellschen Gleichungen (i. S. unserer Definition) stehen; die Gleichungen sind dennoch diophantisch. Die Funktionen $Y_1, Y_2 : I\!N_0^2 \longrightarrow I\!N_0$ definieren wir für $x \geq 2$ durch

$$Y_1(x, n) + Y_2(x, n)\sqrt{x^2 - 1} :\Longleftrightarrow (x + \sqrt{x^2 - 1})^n; \tag{2.39}$$

für $x = 0, 1$ setzen wir einfach $Y_1(x, n) = 1$ und $Y_2(x, n) = 0$.

Die Eigenschaften für Y_1 und Y_2 werden wir nur für $x \geq 2$ betrachten, denn nur in diesem Fall sind $(Y_1(x, n), Y_2(x, n))$ Lösungen von Pellschen Gleichungen. Dem x aus dem vorigen Abschnitt entspricht nun $x + \sqrt{x^2 - 1}$.

Lemma 2.3.3

(i) P_1 und P_2 sind diophantische Relationen.

(ii) Für $x \geq 2$ gilt $Y_1(x, n) + (x^2 - 1)Y_2(x, n) = 1$.

(iii) Für $x \geq 2$ gilt:

$$P_1(y_1, x) \quad \Longleftrightarrow \quad \exists n \in I\!N_0 : y_1 = Y_1(x, n) ,$$
$$P_2(y_2, x) \quad \Longleftrightarrow \quad \exists n \in I\!N_0 : y_2 = Y_2(x, n) .$$

Beweis :

(i) ist sofort klar. (ii) ist auch klar, da für $x \geq 2$ dann $x + \sqrt{x^2 - 1}$ das erzeugende Element der Lösung der Pellschen Gleichung ist und damit $Y_1(x, n) + Y_2(x, n)\sqrt{x^2 - 1}$ auch eine Lösung ist.

Für $P_1(y_1, x)$ ist die Existenz von $y_2 \in I\!N_0$ gefordert, so daß (y_1, y_2) die Pellsche Gleichung löst. Wegen $y_1, y_2 \geq 0$ folgt, daß $y_1 + y_2\sqrt{x^2 - 1} \geq 1$. Deshalb gilt mit Lemma 2.1.9, daß $y_1 + y_2\sqrt{x^2 - 1} = (x + \sqrt{x^2 - 1})^n$ mit $n \geq 0$, und daraus folgt die erste Gleichung in (iii). Die zweite Gleichung folgt analog. □

Die Nummer (iii) der letzten Bemerkung ist nun das Analogon zum vorigen Abschnitt: $P(y, x) \iff \exists n \in I\!N_0 : y = x^n$. Unser nächstes Ziel ist nun, analog dem dortigen Vorgehen eine diophantische Gleichung für Y_1 und Y_2 unter Einbeziehung der Relationen P_1 und P_2 zu entwickeln. Da aber P_1 und P_2 diophantisch sind, sind dann auch Y_1 und Y_2 diophantische Funktionen.

Nun ein Lemma, das im analogen Fall trivial ist:

Lemma 2.3.4 *Es gilt für $x \geq 2$ und $n \pm m \geq 0$:*

$$\begin{aligned} Y_1(x, n \pm m) &= Y_1(x,n)Y_1(x,m) + (x^2-1)Y_2(x,n)Y_2(x,m)\,, \\ Y_2(x, n \pm m) &= \pm Y_1(x,n)Y_2(x,m) + Y_2(x,n)Y_1(x,m)\,. \end{aligned}$$

Beweis :

Wir definieren die Funktionen $\tilde{Y}_1, \tilde{Y}_2$ auf $I\!N_0 \times Z\!\!\!Z$ mittels

$$\tilde{Y}_1(x,n) + \tilde{Y}_2(x,n)\sqrt{x^2-1} :\Longleftrightarrow (x + \sqrt{x^2-1})^n\,. \tag{2.40}$$

Für $n \geq 0$ stimmt $\tilde{Y}_1(x,n)$ und $\tilde{Y}_2(x,n)$ mit $Y_1(x,n)$ bzw. $Y_2(x,n)$ überein. Weiter gilt für $x \geq 2$:

$$\begin{aligned} \tilde{Y}_1(x,-n) + \tilde{Y}_2(x,-n) &= (x + \sqrt{x^2-1})^{-n} \\ &= (\tilde{Y}_1(x,n) + \tilde{Y}_2(x,n))^{-1} \\ &= \overline{\tilde{Y}_1(x,n) + \tilde{Y}_2(x,n)} \\ &= \tilde{Y}_1(x,n) - \tilde{Y}_2(x,n)\,, \end{aligned}$$

und damit folgt:

$$\begin{aligned} \tilde{Y}_1(x,-n) &= \tilde{Y}_1(x,n)\,, \\ \tilde{Y}_2(x,-n) &= -\tilde{Y}_2(x,n)\,. \end{aligned}$$

Daraus ergibt sich für $n, m \in Z\!\!\!Z$:

$$\begin{aligned} \tilde{Y}_1(x, n \pm m) + \tilde{Y}_2(x, n \pm m)\sqrt{x^2-1} &= (x + \sqrt{x^2-1})^n (x + \sqrt{x^2-1})^{\pm m} \\ &= (\tilde{Y}_1(x,n) + \tilde{Y}_2(x,n)\sqrt{x^2-1}) \times \\ &\quad \times (\tilde{Y}_1(x,\pm m) + \tilde{Y}_2(x,\pm m)\sqrt{x^2-1}) \\ &= (\tilde{Y}_1(x,n) + \tilde{Y}_2(x,n)\sqrt{x^2-1}) \times \\ &\quad \times (\tilde{Y}_1(x,m) \pm \tilde{Y}_2(x,m)\sqrt{x^2-1})\,. \end{aligned}$$

Für $n, m \in I\!N_0$ und $n \pm m \geq 0$ können wir wieder $\tilde{Y}_1, \tilde{Y}_2$ durch Y_1 bzw. Y_2 ersetzen, und wir erhalten die behauptete Gleichung. □

Einige Male werden Monotonieeigenschaften der Funktionen Y_1, Y_2 verwendet.

Lemma 2.3.5 *Es gilt für $n, n' \in I\!N_0$ mit $n \leq n'$ und $x \geq 2$*

$$\begin{aligned} Y_1(x,n) &\leq Y_1(x,n')\,, \\ Y_2(x,n) &\leq Y_2(x,n')\,. \end{aligned}$$

Beweis :

Die Ungleichungen ergeben sich per Induktion mittels der Additionstheoreme und der daraus folgenden Ungleichungen:

$$Y_1(x,n+1) = xY_1(x,n) + (x^2-1)Y_2(x,n) \geq Y_1(x,n)$$

und

$$Y_2(x,n+1) = xY_2(x,n) + Y_1(x,n) \geq Y_2(x,n)\,.$$

□

Wir gehen nun analog zum vorigen Abschnitt Stufe für Stufe vor, wobei die entsprechenden Beziehungen entwickelt werden. Wir werden hierbei im wesentlichen immer das x von früher durch $x + \sqrt{x^2 - 1}$ zu ersetzen haben. Das Ziel ist, die Gleichungen

$$y_1 = Y_1(x, n) \wedge y_2 = Y_2(x, n) \tag{2.41}$$

auszudrücken. Eine davon reicht aus, da sich jeweils eine mittels der Pellschen Gleichung aus der anderen ergibt. Es wird sich als etwas günstiger erweisen, zu versuchen $y_2 = Y_2(x, n)$ statt $y_1 = Y_1(x, n)$ diophantisch auszudrücken.

Wir arbeiten bei der Herleitung der entsprechenden Gleichungen wahlweise in $\mathbb{R}$ oder in $\mathbb{Z}[\sqrt{d}]$.

Zunächst analog zu Lemma 2.2.3

Lemma 2.3.6 *Für $x, n \in \mathbb{N}_0$ und $x \geq 2$ gilt: $Y_1(x, n) - 1, Y_2(x, n) \geq n$.*

Beweis :

Für $n = 0$ ist $Y_1(x, 0) = 1$ und $Y_2(x, 0) = 0$. Sei also im weiteren $n \geq 1$. Zunächst gilt unter Verwendung von Lemma 2.2.3

$$Y_1(x, n) = \left\lceil (x + \sqrt{x^2 - 1})^n / 2 \right\rceil > (2x - 1)^n / 2 > 2^{n-1} \geq n\,, \tag{2.42}$$

also $Y_1(x, n) \geq n + 1$. Weiter gilt wegen Lemma 2.3.4

$$Y_2(x, n) = Y_1(x, n - 1) + xY_2(x, n - 1) \geq Y_1(x, n - 1) \geq n\,.$$

□

In den folgenden Stufen 1–5 setzen wir generell $\underline{x \geq 2}$ voraus.

2.3.1 Stufe 1

Entsprechend der Entwicklung von x^n in Potenzen von $x - 1$, schreiben wir nun:

$$\begin{aligned} \left(x + \sqrt{x^2 - 1}\right)^n &= \left(\left(x - 1 + \sqrt{x^2 - 1}\right) + 1\right)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \left(x - 1 + \sqrt{(x + 1)(x - 1)}\right)^i . \end{aligned} \tag{2.43}$$

Der für uns relevante Term steckt im Summanden für $i = 1$. Für $i \geq 2$ schreiben wir zunächst:

$$\begin{aligned} &\left(x - 1 + \sqrt{(x + 1)(x - 1)}\right)^i \\ &\quad = \left(x - 1 + \sqrt{(x + 1)(x - 1)}\right)^2 \left(x - 1 + \sqrt{(x + 1)(x - 1)}\right)^{i-2} \\ &\quad = (x - 1) \left(2x + 2\sqrt{(x + 1)(x - 1)}\right) \left(x - 1 + \sqrt{(x + 1)(x - 1)}\right)^{i-2} \\ &\quad =: \hat{y}_1 + \hat{y}_2 \sqrt{x^2 - 1}\,. \end{aligned}$$

Wegen dem ausgeklammerten Vorfaktor ist sowohl $\hat{y}_1$ als auch $\hat{y}_2$ durch $x - 1$ teilbar. Verwendet man dies in der komponentenweise geschriebenen Gleichung 2.43, so erhält man

$$Y_1(x, n) \equiv 1 + n(x - 1) \equiv 1 \pmod{x - 1}\,, \tag{2.44}$$

$$Y_2(x, n) \equiv n \pmod{x - 1}\,. \tag{2.45}$$

Die zweite Gleichung ist nun das Analogon zu 2.14. Interessanterweise mußten wir im Unterschied zur Herleitung von 2.14 nur bis zur ersten Potenz entwickeln. Das liegt nun daran, daß $Y_2(x,n)\sqrt{x^2-1} \simeq xY_2(x,n)$ gewissermaßen schon den ersten Grad in der Entwicklung nach Potenzen von x beinhaltet.

Wir schreiben also

$$y_2 = Y_2(x,n) \Longrightarrow \begin{cases} \quad (1a') & P_2(y_2,x) \\ \wedge(1b') & y_2 \equiv n \pmod{x-1} \\ \wedge(1c') & n \le y_2\,. \end{cases} \tag{1'}$$

Beweis :

(1a′) ist klar. (1b′) ergibt sich aus (2.45). (1c′) ergibt sich aus Gleichung (2.3.6). □

2.3.2 Stufe 2

Wir definieren hier analog eine Relation Q_2 durch

$$Q_2(y_2^{(1)},x^{(1)},y_2^{(2)},x^{(2)}) :\Longleftrightarrow \exists m \in \mathbb{N} \begin{cases} \quad y_2^{(1)} = Y_2(x^{(1)},m) \\ \wedge \quad y_2^{(2)} = Y_2(x^{(2)},m)\,. \end{cases} \tag{2.46}$$

Im Analogon war es uns möglich, die Gleichheit der Exponenten von zwei Potenzen durch den Logarithmus auszudrücken, ohne zusätzlich zu fordern, daß zwei Potenzen vorliegen. Letzteres wurde dann explizit gefordert. Dies wäre auch hier möglich, die Formeln aber etwas kompliziert, ohne daß sie etwas Wesentliches aussagen würden. Deshalb fordern wir die explizite Gestalt von $y_2^{(1)}$ und $y_2^{(2)}$ schon in Q_2; fordern dies aber noch einmal explizit, da Q_2 in den weiteren Stufen durch eine schwächere Relation ersetzt und die explizite Forderung notwendig wird.[8]

Wir schreiben nun

$$y_2 = Y_2(x,n) \Longleftrightarrow \exists \bar{y}_2, \bar{x} \quad \text{mit} \quad \begin{cases} \quad (2a') & P_2(y_2,x) \\ \wedge(2b') & P_2(\bar{y}_2,\bar{x}) \\ \wedge(2c') & Q_2(\bar{y}_2,\bar{x},y_2,x) \\ \wedge(2d') & \bar{y}_2 \equiv n \pmod{\bar{x}-1} \\ \wedge(2e') & \bar{x} \ge y_2+2 \\ \wedge(2f') & n \le y_2\,. \end{cases} \tag{2'}$$

Beweis :

„⇒“: (2a′) ist klar. Wir setzen $\bar{x} := y_2 + 2 \ge 2$, damit gilt (2e′). Weiterhin definieren wir $\bar{y}_2 := Y_2(\bar{x},n)$, damit gilt (2b′) und (2c′). (2d′) ergibt sich aus (2.45). (2f′) ergibt sich aus Lemma 2.3.6.

„⇐“: Aus (2a′) und (2b′) folgt: Es existieren $k,\ell \in \mathbb{N}_0$ mit $y_2 = Y_2(x,k)$ und $\bar{y}_2 = Y_2(\bar{x},\ell)$. Wegen (2c) folgt $k = \ell$. Also gilt $\bar{y}_2 = Y_2(\bar{x},k)$ und deswegen $\bar{y}_2 \equiv k \pmod{\bar{x}-1}$ $(*)$. Zunächst folgt daraus mit (2d′) $k \equiv n \pmod{\bar{x}-1}$. Aus $y_2 = Y_2(x,k)$ ergibt sich wegen Lemma 2.3.6 auch $k \le y_2$. Zusammen mit (2f′) gilt dann $k,n \le y_2 < \bar{x}-1$. Wendet man darauf $(*)$ an, so ergibt sich $k = n$, also $y_2 = Y_2(x,n)$.

□

[8] Geht man analog der hier verwendeten Vorgehensweise im Analogon vor, so wäre dort zu fordern: $Q(y_1,x_1,y_2,x_2) :\Longleftrightarrow (\exists m \in \mathbb{N} : y_1 = x_1^m \wedge y_2 = x_2^m)$.

2.3.3 Stufe 3

Nun wird Q_2 durch $\overline{Q}_2$ ersetzt. Damit wir nicht in einer der weiteren Stufen $\overline{Q}_2$ wieder umdefinieren müssen, machen wir gegenüber dem Vorgehen in Abschnitt 2.2.3 eine kleine Änderung, nämlich ein zusätzliches $\pm$ auf der einen Seite der Kongruenz. Wir definieren $\overline{Q}_2$ durch

$$\overline{Q}_2(y_2^{(1)}, x^{(1)}, y_2^{(2)}, x^{(2)}, z) :\Longleftrightarrow \exists m_1, m_2 \in I\!N \begin{cases} \quad y_2^{(1)} = Y_2(x^{(1)}, m_1) \\ \wedge \quad y_2^{(2)} = Y_2(x^{(2)}, m_2) \\ \wedge \quad m_1 \equiv \pm m_2 \pmod{z}\,. \end{cases} \tag{2.47}$$

Damit schreiben wir nun

$$y_2 = Y_2(x,n) \Longleftrightarrow \exists \bar{y}_2, \bar{x}, z \quad \text{mit} \quad \begin{cases} \quad (3\text{a}') & P_2(y_2, x) \\ \wedge(3\text{b}') & P(\bar{y}_2, \bar{x}) \\ \wedge(3\text{c}') & \overline{Q}_2(\bar{y}_2, \bar{x}, y_2, x, 2z) \\ \wedge(3\text{d}') & \bar{y}_2 \equiv n \pmod{2z} \\ \wedge(3\text{e}') & n, y_2 \leq z \\ \wedge(3\text{f}') & \bar{x} \equiv 1 \pmod{2z}, \bar{x} \geq 2\,. \end{cases} \tag{3'}$$

Die Moduln in den Kongruenzen (3d′) und (3f′) wurden durch $2z$ ersetzt, um die verringerte Anforderung an $\overline{Q}_2$ auszugleichen. Wie sich aus dem Beweis ergibt, benötigen wir dann nur noch $z \geq y_2, n$ statt $z > y_2, n$.

Der Beweis ist wieder recht einfach:

Beweis :

„⇒“: (3a′) ist klar. Wir setzen $z := y_2 + 1 \geq 1$, $\bar{x} := 2z + 1 \geq 3$ und $\bar{y}_2 := Y_2(\bar{x}, n)$, damit gilt (3b′), (3c′) und (3f′) (in (3c′) sogar mit Gleichheit in der Kongruenzrelation). (3e′) gilt wegen $n \leq y_2 \leq z$.

„⇐“: Aus (3a′) und (3b′) (oder auch (2c′)) folgt: Es existieren $k, \ell \in I\!N$ mit $y_2 = Y_2(x, k)$ und $\bar{y}_2 = Y_2(\bar{x}, \ell)$. Wegen (3c′) folgt $k \equiv \pm\ell \pmod{2z}$. Aus $\bar{y}_2 = Y_2(\bar{x}, \ell)$ und (3f′) folgt $\bar{y}_2 \equiv \ell \pmod{\bar{x} - 1}$, mit (3f′) folgt $\bar{y}_2 \equiv \ell \pmod{2z}$, und mit (3d′) folgt $\ell \equiv n \pmod{2z}$.

Insgesamt ergibt sich damit $k \equiv \pm n \pmod{2z}$ $(*)$. Aus $y_2 = Y_2(x, k)$ ergibt sich $k \leq y_2 \leq z$. Zusammen mit (3e′) gilt dann $k, n \leq y_2 \leq z$. Gilt $k \equiv n \pmod{2z}$ in $(*)$, so ergibt sich dann $k = n$; gilt $k \equiv -n \pmod{2z}$, so ergibt sich $2z | k + n$, und wegen $k + n \leq 2z$ ergibt sich $k + n = 0 \Longrightarrow k = n = 0$ oder $k + n = 2z \Longrightarrow k = n = z$. In jedem Fall ist also $k = n$, also $y_2 = Y_2(x, n)$.

□

Stufe 2 und 3 waren fast reine Umschreibungen der entsprechenden Stufen des Analogons. Bei der nächsten Stufe muß etwas mehr Arbeit geleistet werden.

2.3.4 Stufe 4

Der im vorigen Abschnitt verwendeten Äquivalenz liegt die Gleichung $x^n \equiv -1 \pmod{x^n + 1}$ zugrunde.

Wir wollen dies nun etwas genauer formulieren. Die Abbildung $E : n \mapsto x^n$ ist ein Homomorphismus zwischen der additiven Halbgruppe $I\!N_0$ und der multiplikativen Halbgruppe der nichtnegativen Potenzen von x. Verknüpft mit einer Restklassenabbildung modulo $q \in I\!N$ ergibt das einen Halbgruppenhomomorphismus ρ von der additiven Halbgruppe $\mathbb{N}$ auf die multiplikative Halbgruppe $\mathbb{Z}_q$. Ist weiter noch $(q,x)=1$, so bildet ρ dann $\mathbb{N}$ sogar auf $\mathbb{Z}_q^\times$ ab, denn in diesem Fall ist $x \in \mathbb{Z}_q^\times$ und damit auch die Potenzen von x (modulo q). Sei im folgenden nun $(q,x)=1$ vorausgesetzt.

Es seien im weiteren $n, n_0, m, m', \ell, k \in \mathbb{N}$. Ist nun $\rho(n)=1$, so folgt aus $m \equiv m' \pmod{n}$ die Gleichung $\rho(m)=\rho(m')$, d. h. $E(m) \equiv E(m') \pmod{q}$. Denn sei o. E. $m = m' + kn$, so folgt $\rho(m) = \rho(n)^k \rho(m') = 1^k \rho(m') = \rho(m')$.

Ist nun $n_0 > 0$ minimal mit $\rho(n_0) = 1$, so folgt aus $\rho(m) = \rho(m')$ die Kongruenz $m \equiv m' \pmod{n_0}$. Denn sei o. E. $m = m' + kn_0 + \ell$ mit $\ell < n_0$. Dann gilt $\rho(m) = \rho(m'+\ell) = \rho(m')\rho(\ell) = \rho(m')$. Wegen $(q,x)=1$ ist $\rho(\mathbb{N})$ eine multiplikative Gruppe und somit $\rho(\ell)=1$. Wegen $\ell < n_0$ und der Minimalitätseigenschaft von n_0 gilt damit $\ell = 0$, d. h. $m \equiv m' \pmod{n_0}$.

Zusammenfassend erhält man

$$m \equiv m' \pmod{n_0} \Longleftrightarrow \rho(m) = \rho(m')\,. \tag{2.48}$$

Wir wenden dies auf die Lösungen der Pellschen Gleichung an, dargestellt als Elemente von $\mathbb{Z}[\sqrt{x^2-1}]$. Die Abbildung $E' : n \mapsto (x + \sqrt{x^2})^n$ ist wieder multiplikativ. Man wünscht sich nun eine Restklassenabbildung in der Form von Lemma 2.1.11, die verknüpft mit E', ein bekanntes n_0 auf $1 \in \mathbb{Z}[\sqrt{x^2-1}]$ abbildet, mit dem Zusatz, daß n_0 minimal mit dieser Eigenschaft ist. Als Restklassenabbildung verwendet man am einfachsten die in Lemma 2.1.11 definierte (also die komponentenweise) Restklassenabbildung.

Geht man von der Pellschen Gleichung aus, so erhält man

$$\begin{aligned} Y_1(x,n)^2 &\equiv 1 \pmod{Y_2(x,n)}\,, && (2.49)\\ Y_2(x,n) &\equiv 0 \pmod{Y_2(x,n)}\,. && (2.50) \end{aligned}$$

Stände nun in der ersten Zeile kein Quadrat, so hätte die komponentenweise Restklassenabbildung modulo $Y_2(x,n)$ die gewünschte Wirkung.

Um nun das Quadrat zu eleminieren, liegt es nahe, das Quadrat auf $Y_1(x,n)+Y_2(x,n)\sqrt{x^2-1}$ zu expandieren.

Man schreibt also:

$$(Y_1(x,n) + Y_2(x,n)\sqrt{x^2-1})^2 = Y_1(x,n)^2 + (x^2-1)Y_2(x,n)^2 + 2Y_2(x,n)Y_1(x,n)\sqrt{x^2-1}\,.$$

Andererseits ist

$$(Y_1(x,n) + Y_2(x,n)\sqrt{x^2-1})^2 = (x + \sqrt{x^2-1})^{2n} = Y_1(x,2n) + Y_2(x,2n)\sqrt{x^2-1}\,. \tag{2.51}$$

Mittels 2.49 und 2.50 liefert dies

$$\begin{aligned} Y_1(x,2n) &\equiv 1 \pmod{Y_2(x,n)}\,, && (2.52)\\ Y_2(x,2n) &\equiv 0 \pmod{Y_2(x,n)}\,. && (2.53) \end{aligned}$$

Das Problem ist hier, daß ein $m < 2n$ existieren kann mit $Y_1(x,m) \equiv 1 \pmod{Y_2(x,n)}$ und $Y_2(x,m) \equiv 0 \pmod{Y_2(x,n)}$, d. h. die geforderte Minimalitätseigenschaft ist nicht gewahrt. Dies liegt nun an $Y_2(x,n) < Y_1(x,n)$. Es wäre also besser, Kongruenzen modulo $Y_1(x,n)$ zu betrachten.

Dies gelingt, indem man nochmals $Y_1(x,2n)+Y_2(x,2n)\sqrt{x^2-1}$ berechnet, $Y_1(x,n)$ herauszieht und dann die Pellsche Gleichung einsetzt.

$$\begin{aligned}
Y_1(x,2n)+Y_2(x,2n)\sqrt{x^2-1} &= (Y_1(x,n)+Y_2(x,n)\sqrt{x^2-1})^2 \\
&= Y_1(x,n)^2+(x^2-1)Y_2(x,n)^2+2Y_1(x,n)Y_2(x,n)\sqrt{x^2-1} \\
&= 2Y_1(x,n)^2-1+2Y_1(x,n)Y_2(x,n)\sqrt{x^2-1} \\
&= -1+Y_1(x,n)(2Y_1(x,n)+2Y_2(x,n)\sqrt{x^2-1})\,.
\end{aligned}$$

Liest man dies modulo $Y_1(x,n)$, so erhält man

$$\begin{aligned}
Y_1(x,2n) &\equiv -1 \pmod{Y_1(x,n)}\,, && (2.54)\\
Y_2(x,2n) &\equiv 0 \pmod{Y_1(x,n)}\,. && (2.55)
\end{aligned}$$

Die -1 statt 1 wird etwas stören, allerdings nicht allzusehr, da $\{-1,1\}$ eine multiplikative Untergruppe in $\mathbb{Z}_{Y_1(x,n)}[\sqrt{x^2-1}]$ bildet und damit obige Prinzipien nicht völlig wertlos sind.

Wichtig ist nun, daß die Minimalitätseigenschaft gilt, d. h. sei $m>0$, dann folgt aus $Y_1(x,m)\equiv\pm1 \pmod{Y_1(x,n)}$ und $Y_2(x,m)\equiv 0 \pmod{Y_1(x,n)}$ $m\geq 2n$. Denn aus $Y_2(x,m)\equiv 0 \pmod{Y_1(x,n)}$ folgt wegen $Y_2(x,n)<Y_1(x,n)$ und $m>0$ die Ungleichung $m>n$. Dann gilt $Y_2(x,m)=Y_2(x,m-n+n)=Y_1(x,m-n)Y_2(x,n)+Y_1(x,n)Y_2(x,m-n)\equiv Y_1(x,m-n)Y_2(x,n) \pmod{Y_1(x,n)}$. Wegen $Y_2(x,n)$ teilerfremd zu $Y_1(x,n)$ (Pellsche Gleichung) und $Y_1(x,n)|Y_2(x,m)$ (Voraussetzung), folgt $Y_1(x,n)|Y_1(x,m-n)$ und daraus entweder $Y_1(x,m-n)=0$ oder $Y_1(x,m-n)\geq Y_1(x,n)$. Ersteres geht nicht wegen $m>n$, das zweite führt zu $m-n\geq n$ bzw. $m\geq 2n$, was zu beweisen war.

Wir haben also den gesuchten Modul gefunden und können damit E' mit $\psi_{Y_1(x,n)}$ entsprechend Lemma 2.1.11 verknüpfen; damit erhält man entsprechend (2.48) oder mittels den Additionstheoremen zusammen mit den Kongruenzen (2.54) und (2.55) zunächst die folgende Implikation

$$k\equiv m \pmod{2\ell} \Longrightarrow Y_2(x,k)\equiv\pm Y_2(x,m) \pmod{Y_1(x,\ell)}\,. \tag{2.56}$$

Laut Additionstheoremen können wir dasselbe auch für $k\equiv -m \pmod{2\ell}$ zeigen. Dies legt mittels der Minimalitätseigenschaft folgende Vermutung nahe.

$$k\equiv\pm m \pmod{2\ell} \Longleftrightarrow Y_2(x,k)\equiv\pm Y_2(x,m) \pmod{Y_1(x,\ell)}\,. \tag{2.57}$$

Die Übertragung von (2.48) auf unseren Fall stößt in der Richtung von rechts nach links auf einige Schwierigkeiten. Weiterhin benötigt man auf der rechten Seite von (2.57) zusätzlich die Gleichung $Y_1(x,k)\equiv\pm Y_2(x,m) \pmod{Y_1(x,\ell)}$. Tatsächlich ist diese Kongruenz unnötig. Der Beweis von (2.57) läßt sich deshalb einfacher führen, er wird in Lemma 2.3.7 gegeben. Diese Betrachtungen hier waren insofern wertvoll, daß sie zu dieser Äquivalenz hingeführt haben, der Beweis ist dann nicht weiter schwierig.

Nun fehlt uns noch das Entsprechende beim Basiswechsel. Dies ist aber sehr einfach, denn

$$Y_2(x_2,n)\equiv Y_2(x_1,n) \pmod{x_2-x_1} \tag{2.58}$$

gilt, weil $Y_2(x,n)$ für festes n ein Polynom in x ist, und da für die einzelnen Monome die Kongruenz gilt, so gilt sie auch für das ganze Polynom.

Da wir in (2.57) als Modul $Y_1(x,\ell)$ stehen haben, liegt es nahe, entsprechend der Relation R des vorigen Abschnitts die Relation R_1 durch

$$R_1(\tilde{y}_1,x,\ell) :\Longleftrightarrow \exists m>0 \text{ mit } \tilde{y}_1=Y_1(x,m)\wedge \ell|m \tag{2.59}$$

zu definieren.

Zur Berücksichtigung des Basiswechsels benötigen wir noch $\tilde{y}_1|\bar{x}-x$. Fügen wir diese Beziehung auf der rechten Seite von (3′) hinzu (damit haben wir später dafür zu sorgen, daß die Implikation von links nach rechts noch möglich ist), so können wir $\overline{Q}_2$ zusammen mit anderen Relationen mittels R_1 und diophantischen Relationen umschreiben:

$$\exists z : \left\{ \begin{array}{ll} (3a') & P_2(y_2, x) \\ \wedge(3b') & P_2(\bar{y}_2, \bar{x}) \\ \wedge(3c') & \overline{Q}_2(y_2, x, \bar{y}_2, \bar{x}, z) \\ \wedge(3e_2') & z \geq 2y_2 \\ \wedge(4e_2') & \bar{x} \equiv x \pmod{Y_1(x,z)}\,. \end{array} \right\} \iff \exists \bar{z}, \tilde{y}_1 \left\{ \begin{array}{ll} (4a') & P_2(y, x) \\ \wedge(4b') & P(\bar{y}_2, \bar{x}) \\ \wedge(4c') & R_1(\tilde{y}_1, x, \bar{z}) \\ \wedge(4d') & \bar{y}_2 \equiv \pm y_2 \pmod{\tilde{y}_1} \\ \wedge(4e') & \bar{x} \equiv x \pmod{\tilde{y}_1} \\ \wedge(4f') & \bar{z} \geq y_2 \end{array} \right. \qquad (4')$$

Wir wollen dies nun noch beweisen:

Beweis :

„⇒“: (4a′) und (4b′) sind direkt übernommen. (4a′) und (4b′) ergeben $\exists k, \ell$ und $y_2 = Y_2(x,k)$, $\bar{y}_2 = Y_2(\bar{x}, \ell)$. Wir setzen $\bar{z} := z$ und $\tilde{y}_1 = Y_1(x, \bar{z})$. Damit gilt (4c′), (4f′) und (4e′). (3c′) impliziert $k \equiv \pm\ell \pmod{z}$. Damit ergibt sich über die Beziehung (2.57) (in der Richtung von rechts nach links) die Beziehung (4d′).

„⇐“: (3a′), (3b′) sind direkt übernommen. (3a′) und (3b′) ergeben wieder $\exists k, \ell$ und $y_2 = Y_2(x,k)$, $\bar{y}_2 = Y_2(\bar{x}, \ell)$. Das ergibt mit (2.58) $\bar{y}_2 = Y_2(\bar{x}, \ell) \equiv Y_2(x, k) \pmod{\bar{x} - x}$ und mit (4e′) ergibt sich $\bar{y}_2 \equiv Y_2(x, \ell) \pmod{\tilde{y}_1}$. Mit (4d′) ergibt sich dann $Y_2(x,\ell) \equiv \pm Y_2(x,k) \pmod{\tilde{y}_1}$. Mittels (4c′) ergibt sich $\exists m$ mit $\tilde{y}_1 = Y_1(x, m)$, $\bar{z}|m$ und $\bar{z} \geq m$. Wir setzen $z := m$; dann gilt mit (4f′) und $\bar{z} \geq m$ (3e$_2'$). Mit (4e′) ergibt sich dann (4e$_2'$). Man erhält weiter $Y_2(x,\ell) \equiv \pm Y_2(x,k) \pmod{x^m + 1}$, und mit (2.57) ergibt sich $\ell \equiv \pm k \pmod{2m}$. Wegen $m = z$ ergibt sich dann (3c′).

□

2.3.5 Stufe 5

In der Entsprechung wurde die Basis x durch eine Basis, die eine Potenz der früheren Basis war, ersetzt und die Kongruenz (2.14) verwendet. Es taucht die Frage auf, durch was wir nun x ersetzen. Im einfachsten Falle könnten $Y_1(x,k)$ oder $Y_2(x,k)$ zum Erfolg führen. Tatsächlich findet man schnell eine ähnliche Relation:

$$\begin{aligned} Y_1(Y_1(x,k),n) + Y_2(Y_1(x,k),n)\sqrt{Y_1^2(x,k)-1} &= \left(Y_1(x,k) + \sqrt{Y_1^2(x,k)-1}\right)^n \\ &= \left(Y_1(x,k) + \sqrt{(x^2-1)Y_2^2(x,k)}\right)^n \\ &= \left(Y_1(x,k) + Y_2(x,k)\sqrt{x^2-1}\right)^n \\ &= \left(x + \sqrt{x^2-1}\right)^{kn} \\ &= Y_1(x,kn) + Y_2(x,kn)\sqrt{x^2-1}\,. \end{aligned}$$

Diese Rechnung liefert wegen $\sqrt{Y_1^2(x,k)-1} = Y_2(x,k)\sqrt{x^2-1}$ die Gleichung

$$Y_2(x, kn) = Y_2(Y_1(x,k), n)Y_2(x,k)\,. \qquad (2.60)$$

Wendet man darauf $Y_2(x',n) \equiv n \pmod{x'-1}$ (2.45) an, so erhält man die Beziehung $Y_2(Y_1(x,k),n) \equiv n \pmod{Y_1(x,k)-1}$ und daraus $Y_2(Y_1(x,k),n) \equiv 0 \pmod{Y_1(x,k)-1} \iff Y_1(x,k)-1|n$ oder umgeschrieben $Y_1(x,k)-1|Y_2(Y_1(x,k),n) \iff Y_1(x,k)-1|n$.

Mit dieser Beziehung lassen sich allerdings die entsprechend benötigten äquivalenten Gleichungen nicht erfüllen.

Deshalb benötigen wir eine ähnliche Beziehung wie (2.45), nur eben statt $x'-1$ ein größeres Modul. Es läßt sich z. B. mittels (2.45) eine ähnliche Beziehung nur mit $x'+1$ beweisen, und dieses läßt sich mit der Kongruenz modulo $x'-1$ kombinieren.

Wir werden aber direkt auf ähnlichem Weg wie in Abschnitt 2.3.1 vorgehen, allerdings werden wir Kongruenzen modulo x^2-1 untersuchen. Wir betrachten zunächst $Y_1(x,2k) + Y_2(x,2k)\sqrt{x^2-1}$ unter Verwendung von Lemma 2.1.11:

$$\begin{aligned}
Y_1(x,2k) + Y_2(x,2k)\sqrt{x^2-1} &= (x+\sqrt{x^2-1})^{2k} \\
&= (2x^2-1+2x\sqrt{x^2-1})^k \\
&\equiv (1+2x\sqrt{x^2-1})^k \\
&= 1+2xk\sqrt{x^2-1}+\binom{k}{2}(x^2-1)4x^2+\ldots \\
&\equiv 1+2xk\sqrt{x^2-1} \pmod{x^2-1}\,.
\end{aligned}$$

Für $Y_1(x,2k+1)+Y_2(x,2k+1)\sqrt{x^2-1}$ erhält man dann entsprechend:

$$\begin{aligned}
Y_1(x,2k+1) + Y_2(x,2k+1)\sqrt{x^2-1} &= (x+\sqrt{x^2-1})^{2k}(x+\sqrt{x^2-1}) \\
&\equiv 1+2xk\sqrt{x^2-1}(x+\sqrt{x^2-1}) \\
&= x+2xk(x^2-1)+(2x^2k+1)\sqrt{x^2-1} \\
&\equiv x+(2k+1)\sqrt{x^2-1} \pmod{x^2-1}\,.
\end{aligned}$$

Damit erhält man ingesamt

$$Y_2(x,k) \equiv \left\{ \begin{array}{ll} kx & \text{für } k \text{ gerade} \\ k & \text{für } k \text{ ungerade} \end{array} \right\} \pmod{x^2-1}\,. \tag{2.61}$$

Mittels dieser Gleichung erhält man die Kongruenz $Y_2(Y_1(x,n),k) \equiv k \pmod{Y_1(x,n)^2-1}$ bzw. $Y_2(Y_1(x,n),k) \equiv kY_1(x,n) \pmod{Y_1(x,n)^2-1}$, daraus wegen $Y_2(x,n)|Y_1(x,n)^2-1$ (Pellsche Gleichung) die Kongruenz $Y_2(Y_1(x,n),k) \equiv k \pmod{Y_2(x,n)}$ bzw. $Y_2(Y_1(x,n),k) \equiv kY_1(x,n) \pmod{Y_2(x,n)}$. Daraus folgt

$$Y_2(x,n)|Y_2(Y_1(x,n),k) \iff Y_2(x,n)|k\,, \tag{2.62}$$

denn die Implikation von rechts nach links ist klar. Von links nach rechts erhält man zunächst $Y_2(x,n)|k$ direkt, bzw. $Y_2(x,n)|kY_1(x,n)$. Wegen $(Y_1(x,n),Y_2(x,n)) = 1$ (Pellsche Gleichung) erhält man auch im letzeren Falle $Y_2(x,n)|k$.

Multipliziert man die Teilbarkeitsbedingung auf der linken Seite von (2.62) mit $Y_2(x,n)$ und setzt (2.60) ein, so erhält man

$$Y_2(x,n)^2|Y_2(x,kn) \iff Y_2(x,n)|k\,, \tag{2.63}$$

was sich einfach schreiben läßt als

$$Y_2(x,n)^2|Y_2(x,\ell) \iff nY_2(x,n)|\ell\,. \tag{2.64}$$

Damit liegt es nahe für z die Bedingung $P_2(z,x)$ zu fordern. Wir schreiben so das Analogon zu (5):

$$R_1(\tilde{y}_1, x, z) \Longleftarrow \begin{cases} (5a') & \tilde{y}_1^2 - (x^2-1)\tilde{y}_2^2 = 1 \\ \wedge(5b') & P_2(z,x) \\ \wedge(5c') & z^2|\tilde{y}_2, z \geq 1 \\ \wedge(5d') & \tilde{y}_2 \equiv 0 \pmod{z}\,. \end{cases} \qquad (5')$$

Beweis :

Aus (5a′) und (5b′) ergibt sich, daß $\exists k, m \in I\!N_0$ mit $\tilde{y}_1 = Y_1(x,k)$, $\tilde{y}_2 = Y_2(x,k)$, $z = Y_2(x,m)$. Aus (5c′) ergibt sich mittels (2.64) $mz|k$. Damit gilt auch $z|k$ und wegen $z \geq 1$ (s. (5c′)) die linke Seite. □

Da wir hier nur eine Implikation haben, und wir außerdem schon in Stufe 4 auf der rechten Seite von (3′) eine weitere Gleichung einfügten, ist noch zu zeigen, daß man die entsprechenden Gleichungen und Kongruenzen auch erfüllen kann.

Die wesentliche Schwierigkeit ist wie im Abschnitt 2.2 die Erfüllbarkeit von

$$\begin{aligned} \bar{x} &\equiv 1 \pmod{2y_2}\,, \\ \bar{x} &\equiv x \pmod{\tilde{y}_1}\,. \end{aligned}$$

Da aber nach (5c′) dann $y_2^2|\tilde{y}_2$ und aufgrund der Pellschen Gleichung wieder $\tilde{y}_2$ und $\tilde{y}_1$ teilerfremd, so ergibt sich, daß auch y_2 und $\tilde{y}_1$ teilerfremd sind, und damit die beiden Kongruenzen für $\bar{x}$ gelöst werden können.

2.3.6 Der vollständige Beweis

Zu Beginn geben wir die in den Stufen 1–5 entwickelten Beziehungen in einem Lemma an, wobei die Beweise teilweise nicht aus dem vorigen Vorgehen entommen sind, sondern kürzere verwendet werden. In (iii) und (iv) wird zur Verkürzung auf Stufe 5 verwiesen, da die entsprechende Rechnung darin recht kompakt enthalten ist.

Lemma 2.3.7 *Sei $x, y, n, k, m \in I\!N_0$ und $x \geq 2$. Es gelten die folgenden fünf Aussagen*

(i) $Y_2(x,n) \equiv n \pmod{x-1}$.

(ii) $Y_2(x,n) \equiv Y_2(x',n) \pmod{x'-x}$.

(iii) $Y_2(x,n)|Y_2(x,m) \Longleftrightarrow n|m$.

(iv) $Y_2(x,n)^2|Y_2(x,m) \Longleftrightarrow nY_2(x,n)|m$.

(v) $Y_2(x,n) \equiv \pm Y_2(x,m) \pmod{Y_1(x,k)} \Longleftrightarrow n \equiv \pm m \pmod{2k}$.

Beweis :

(i) Wir schreiben unter Verwendung von komponentenweiser Konjugation

$$\begin{aligned} Y_1(x,n) + Y_2(x,n)\sqrt{x^2-1} &= \\ &= \left(x + \sqrt{x^2-1}\right)^n \\ &= \left(\left(x - 1 + \sqrt{x^2-1}\right) + 1\right)^n \end{aligned} \qquad (2.65)$$

$$\begin{aligned}
&= \sum_{i=0}^{n} \binom{n}{i} \left(x - 1 + \sqrt{(x+1)(x-1)}\right)^i \\
&= 1 + n\left(x - 1 + \sqrt{x^2-1}\right) \\
&\quad + \left(x - 1 + \sqrt{(x+1)(x-1)}\right)^2 \sum_{i=2}^{n} \binom{n}{i} \left(x - 1 + \sqrt{x^2-1}\right)^{i-2} \\
&= 1 + n(x-1) + n\sqrt{x^2-1} + (x-1)(2x + 2\sqrt{x^2-1}) \sum_{i=2}^{n} \dots \\
&\equiv 1 + n \pmod{x-1}\,. \qquad (2.66)
\end{aligned}$$

(ii) Für konstantes n ist $Y_2(x,n)$ ein Polynom in x, damit folgt die Kongruenz aus Lemma 2.2.4(ii).

(iii) „$\Leftarrow$“: Aus $n|m$ folgt $\exists \ell$ mit $m = \ell n$. Dann ist mit Gleichung (2.60) $Y_2(x,m) = Y_2(x,\ell n) = Y_2(Y_1(x,n),\ell) Y_2(x,n)$ und damit $Y_2(x,n)|Y_2(x,m)$.

(iii) „$\Rightarrow$“: Sei $m = \ell n + m'$ und $m' < n$. Dann gilt aufgrund der Additionstheoreme $Y_2(x,m) = Y_2(x,\ell n)Y_1(x,m') + Y_1(x,\ell n)Y_2(x,m')$. Nun gilt aufgrund der schon gezeigten (iii)„$\Leftarrow$“ die Beziehung $Y_2(x,n)|Y_2(x,\ell n)$. Nach Voraussetzung folgt dann $Y_2(x,n)|Y_1(x,\ell n)\cdot Y_2(x,m')$ $(*)$. Da wegen der Pellschen Gleichung $Y_1(x,\ell n)$ und $Y_2(x,\ell n)$ teilerfremd sind und $Y_2(x,n)|Y_2(x,\ell n)$, folgt aus $(*)$ $Y_2(x,n)|Y_2(x,m')$. Aufgrund der Monotonie folgt $m' = 0$ oder $m' \geq n$. Wegen $m' < n$ folgt dann aber $m' = 0$ und damit $n|m$.

(iv) Wir verweisen auf (2.64).

(v) „$\Leftarrow$“: Ohne Einschränkung können wir annehmen, daß $n > m$ ist, d. h. es existiert $\ell \in \mathbb{N}_0$ mit $n = 2\ell k \pm m$.

Zunächst liefert das Additionstheorem und die Pellsche Gleichung

$$Y_1(x,2k) = Y_1(x,k)^2 + (x^2-1)Y_2(x,k)^2 = 2Y_1(x,k)^2 - 1 \equiv -1 \pmod{Y_1(x,k)}$$

und

$$Y_2(x,2k) = 2Y_1(x,k)Y_2(x,k) \equiv 0 \pmod{Y_1(x,k)}\,. \qquad (2.67)$$

Weiter gilt für $\ell \in \mathbb{N}_0$ wegen 2.1.11

$$\begin{aligned}
Y_1(x,2k\ell) + Y_2(x,2k\ell)\sqrt{x^2-1} &= (Y_1(x,2k) + Y_2(x,2k)\sqrt{x^2-1})^\ell \\
&\equiv (-1)^\ell = \pm 1 \pmod{Y_1(x,k)}\,.
\end{aligned}$$

Also gilt

$$\begin{aligned}
Y_1(x,2k\ell) &\equiv \pm 1 \pmod{Y_1(x,k)}\,, \\
Y_2(x,2k\ell) &\equiv 0 \pmod{Y_1(x,k)}\,.
\end{aligned}$$

Dann liefert das Additionstheorem

$$\begin{aligned}
Y_2(x,n) &= Y_2(x,2\ell k \pm m) \\
&= \pm Y_1(x,2\ell k)Y_2(x,m) + Y_2(x,2\ell k)Y_1(x,m) \\
&\equiv \pm Y_2(x,m) \pmod{Y_1(x,k)}\,.
\end{aligned}$$

(v) „$\Rightarrow$“: Sei $n = 2\ell_1 k + n'$ und $m = 2\ell_2 k + m'$ mit $\ell_1, \ell_2 \in \mathbb{N}_0$ und $n', m' < 2k$. Dann gilt wegen dem schon bewiesenen (v)„$\Leftarrow$“: $Y_2(x, n') \equiv \pm Y_2(x, m') \pmod{Y_1(x,k)}$. Für $k \le n' < 2k$ sei $n'' := 2k - n'$, sonst $n'' := n'$. Entsprechend sei m'' definiert. Dann gilt $n'', m'' \le k$, und wegen (v)„$\Leftarrow$“ gilt wieder $Y_2(x, n'') \equiv \pm Y_2(x, m'') \pmod{Y_1(x,k)}$. Damit folgt $Y_1(x,k) | Y_2(x,n'') \pm Y_2(x,m'')$ (*).

Gilt nun $n'' \ne m''$, so folgt $n'' < k$ oder $m'' < k$. Damit folgt $|Y_2(x,n'') \pm Y_2(x,m'')| \le Y_2(x,k) + Y_2(x,k-1)$. Aus dem Additionstheorem folgt $Y_2(x,k) > xY_2(x,k-1)$, also $Y_2(x,k-1) < Y_2(x,k)/x$. Damit ist $Y_2(x,k) + Y_2(x,k-1) < \frac{x+1}{x} Y_2(x,k)$. Mittels der Pellschen Gleichung folgt $Y_2(x,k) < Y_1(x,k)/\sqrt{x^2-1}$. Damit folgt $Y_2(x,k) + Y_2(x,k-1) < \frac{x+1}{x\sqrt{x^2-1}} Y_2(x,k) < (\frac{1}{\sqrt{x^2-1}} + \frac{1}{x\sqrt{x^2-1}}) Y_2(x,k) < \frac{3}{2\sqrt{3}} Y_2(x,k) < Y_2(x,k)$. (Man beachte $x \ge 2$.) Insgesamt ergibt sich $|Y_2(x,n'') \pm Y_2(x,m'')| < Y_2(x,k)$.

Zusammen mit (*) folgt dann $Y_2(x,n'') \pm Y_2(x,m'') = 0$ also $n'' = m''$, im Widerspruch zur Annahme.

Wir haben also $n'' = m''$, woraus dann nach Definition von n'', m'' folgt, daß $n \equiv \pm m \pmod{2k}$ ist.

□

Mit Lemma 2.3.7 sind wir in der Lage den folgenden Satz zu beweisen:

Satz 2.3.8 *Sei $x, n \in \mathbb{N}_0$ und $x \ge 2$. Dann gilt folgende Äquivalenz:*

$$y_2 = Y_2(x,n) \iff \exists \bar{x}, y_1, \bar{y}_1, \bar{y}_2, \tilde{y}_1, \tilde{y}_2 \in \mathbb{N}_0 \text{ mit } \begin{cases} (6a') & y_1^2 - (x^2-1)y_2^2 = 1 \\ \wedge(6b') & \bar{y}_1^2 - (\bar{x}^2-1)\bar{y}_2^2 = 1 \\ \wedge(6c') & \tilde{y}_1^2 - (x^2-1)\tilde{y}_2^2 = 1 \\ \wedge(6d') & y_2^2 | \tilde{y}_2, \tilde{y}_2 \ge y_2 \\ \wedge(6e') & \bar{x} \equiv 1 \pmod{2y_2} \\ \wedge(6f') & \bar{x} \equiv x \pmod{\tilde{y}_1} \\ \wedge(6g') & \bar{y}_2 \equiv y_2 \pmod{\tilde{y}_1} \\ \wedge(6h') & \bar{y}_2 \equiv n \pmod{2y_2} \\ \wedge(6i') & n \le y_2\,. \end{cases} \qquad (6')$$

Man beachte, daß gegenüber Kongruenz (4d$'$) das $\pm$ fehlt. Dies liegt daran, daß in der Implikation von links nach rechts $\bar{y}_2$ entsprechend definiert werden kann. Im Originalbeweis steht in (6d$'$) $2y_2^2|\tilde{y}_2$. Diese Beziehung wird beim Beweis der Implikation „$\Rightarrow$“ weiterverwendet. Wir verzichten auf diese Vereinfachung der Referenzen.

Beweis :

„$\Rightarrow$“: Setze $y_1 := Y_1(x,n)$; dann gilt (6a$'$). Setze $\tilde{y}_1 := Y_1(x, 2ny_2)$, $\tilde{y}_2 := Y_2(x, 2ny_2)$; dann gilt (6c$'$), und wegen Lemma 2.3.7(iv)„$\Leftarrow$“ folgt $y_2^2|\tilde{y}_2$, also die Teilbarkeitsbeziehung in (6d$'$). Es ist $\tilde{y}_2 = 0$ nur, wenn $y_2 = 0$, damit gilt generell $\tilde{y}_2 \ge y_2$, also die Ungleichung in (6d$'$). Wegen $Y_2(x,2m) = 2Y_1(x,m)Y_2(x,m)$ (Lemma 2.3.4) gilt $2y_2^2|\tilde{y}_2$ und damit $2y_2|\tilde{y}_2$. Aus $(\tilde{y}_1, \tilde{y}_2) = 1$ (Pellsche Gleichung) folgt dann $(\tilde{y}_1, 2y_2) = 1$. Damit folgt weiter, daß $\bar{x}$ so gewählt werden kann, daß (6e$'$) und (6f$'$) erfüllt ist. (Wähle z. B. stärker $\bar{x} \equiv 1 \pmod{\tilde{y})_2^2}$, $\bar{x} \equiv x \pmod{\tilde{y})_1^2}$; unter Verwendung der aus der Pellschen Gleichung abgeleiteten Kongruenz $\tilde{y}_1^2 \equiv 1 \pmod{\tilde{y}_2^2}$ wählt man einfach $\bar{x} = x + \tilde{y}_1^2(\tilde{y}_1^2 - x)$ (für $n = 0$ würde $\bar{x}$ negativ, hier setze man $\bar{x} = 1$, denn $\tilde{y}_1^2 = 1$ und $\bar{x} \equiv x \pmod 1$. Man muß dann die übrigen Beziehungen von Hand nachweisen, da in Lemma 2.3.4 meist $x \ge 2$ vorausgesetzt wird.))

Setze $\bar{y}_1 := Y_1(\bar{x}, n)$, $\bar{y}_2 := Y_2(\bar{x}, n)$; dann gilt (6b′). Wegen (6f′) und Lemma 2.3.7(ii) gilt (6g′). Wegen (6e′) und Lemma 2.3.7(i) gilt (6h′). Schließlich gilt (6i′) wegen Lemma 2.3.6.

„$\Leftarrow$“: Aus (6a′), (6b′) und (6c′) folgt mittels Lemma 2.3.3: $\exists p, q, r \in \mathbb{N}_0$ mit $y_1 = Y_1(x,p)$, $y_2 = Y_2(x,p)$, $\bar{y}_1 = Y_1(x,q)$, $\bar{y}_2 = Y_2(\bar{x},q)$, $\tilde{y}_1 = Y_1(\bar{x},r)$, $\tilde{y}_2 = Y_2(x,r)$. Aus $y_2 = Y_2(x,p)$ folgt mittels Lemma 2.3.6 $p \leq y_2$. Wegen (6i′) folgt $n \leq y_2$. Es reicht nun zu zeigen, daß $p \equiv \pm n \pmod{2y_2}$. Denn gilt $p \equiv n \pmod{2y_2}$, so ergibt sich direkt $p = n$; gilt $p \equiv -n \pmod{2y_2}$, so ergibt sich $2y_2 | p + n$, und wegen $p + n \leq 2y_2$ ergibt sich $k + n = 0 \Longrightarrow k = n = 0$ oder $k + n = 2y_2 \Longrightarrow k = n = y_2$. In jedem Fall ist also $k = n$, also $y_2 = Y_2(x,n)$.

Wegen Lemma 2.3.7(i) folgt aus $\bar{y}_2 = Y_2(\bar{x},q)$ die Kongruenz $\bar{y}_2 \equiv q \pmod{\bar{x}-1}$ und mittels (6e′) $\bar{y}_2 \equiv q \pmod{2y_2}$. Mittels (6h′) folgt damit $q \equiv n \pmod{2y_2}$ $(*_1)$.

Aus (6g′) folgt mittels Lemma 2.3.7(v) $p \equiv \pm q \pmod{2r}$. Aus (6d′) folgt aber $y_2 | r$, also $2y_2 | 2r$ und damit $p \equiv \pm q \pmod{2y_2}$ $(*_2)$.

$(*_1)$ und $(*_2)$ ergeben $p \equiv \pm n \pmod{2y_2}$, was noch zu zeigen war.

□

Korollar 2.3.9 *Die Funktionen Y_1 und Y_2 sind diophantisch.*

Beweis :

Y_2 ist diophantisch, denn wir können schreiben

$$y_2 = Y_2(x,n) \Longleftrightarrow \exists \bar{x}, \bar{y}_1, \bar{y}_2, \tilde{y}_1, \tilde{y}_2 \in \mathbb{N}_0 \text{ mit } \begin{cases} & (x = 0,1 \wedge y_2 = 0) \\ \vee & (x \geq 2 \wedge (6a') \wedge \ldots \wedge (6i')) \,. \end{cases}$$

Auf der rechten Seite stehen nur diophantische Relationen, also ist Y_2 diophantisch. Für Y_1 schreiben wir

$$y_1 = Y_1(x,n) \iff y_1^2 - (x^2-1)Y_2(x,n)^2 - 1 = 0 \,.$$

Für $x = 0,1$ prüft man die Äquivalenz sofort nach.

Für $x \geq 2$ ergibt sich die Implikation von rechts nach links bis auf Vorzeichen aufgrund der Definition von Y_1 und Y_2. Wird die rechte Seite als diophantische Gleichung interpretiert, so folgt $y_1 \in \mathbb{N}_0$. Die Implikation von links nach rechts ist sofort einsichtig.

Damit steht aber auf der rechten Seite eine diophantische Gleichung und damit ist Y_1 diophantisch. □

Mittels diesem Korollar läßt sich im nächsten Abschnitt insbesondere die Exponentialfunktion als diophantisch nachweisen.

2.4 Die diophantische Gleichung für die Exponentialfunktion

Durch den Übergang von der Relation $P(y,x)$ zu $P_1(y_1,x)$ und $P_2(y_2,x)$ haben wir uns eine Schwierigkeit eingehandelt. Denn unser Ziel ist es, die Diophantizität der Exponentialfunktion nachzuweisen. Im vorigen Abschnitt wurde aber nur gezeigt, daß $Y_1(x,n)$ und $Y_2(x,n)$ diophantische Funktionen sind.

Da nun $Y_1(x,n)$ sich annähernd wie eine Exponentialfunktion verhält, und zwar mit einer reellen Basis, muß man quasi die gesuchte Exponentialfunktion durch eine Exponentialfunktion mit einer anderen Basis ausdrücken. Hierzu gehen wir zunächst wieder auf Exponentialfunktionen ganzzahliger Basen zurück.

Die Idee ist ähnlich zu Abschnitt 2.2.1. Wir können nämlich ähnlich wie dort schreiben (mit $x, z \in \mathbb{N}$):

$$\begin{aligned} x^n &= (x-z+z)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} (x-z)^i z^{n-i} \\ &\equiv z^n \pmod{x-z}\,. \end{aligned}$$

Wenn nun gilt $x - z > z^n$, so gilt dann $z^n = \mathrm{rem}(x^n, x-z)$, und wir können schreiben:

$$y = z^n \iff \exists x : \begin{cases} \quad x > z^n + z \\ \wedge \quad y = \mathrm{rem}(x^n, x-z)\,. \end{cases} \tag{2.68}$$

Beweis: Die Richtung von links nach rechts folgt durch $x := y + z + 1$. Umgekehrt folgt aus der zweiten Gleichung der rechten Seite $z^n \equiv y \pmod{x-z}$. Weiter folgt wegen $\mathrm{rem}(x^n, x-z) < x-z$ die Ungleichung $y < x-z$ und wegen der ersten Gleichung auf der rechten Seite $z^n < x-z$. Damit folgt aus der Kongruenz $z^n \equiv y \pmod{x-z}$ die Gleichung $y = z^n$, was zu zeigen war.

Natürlich ist die Äquivalenz etwas eigenartig, da der Term z^n auf der rechten Seite nochmals auftaucht, wesentlich ist aber, daß dies nur zur Abschätzung benötigt wird.

Man kann diese Äquivalenz übrigens auch dazu verwenden, aus der Diophantizität der Funktion $a \mapsto a^n$ die Diophantizität der Funktion $(x,n) \mapsto x^n$ zu gewinnen. Wir führen dies hier nicht aus.

Nun gehen wir zu den Lösungen der Pellschen Gleichungen über und schreiben ähnlich wie in 2.3.1

$$\begin{aligned} Y_1(x,n) + Y_2(x,n)\sqrt{x^2-1} &= (x + \sqrt{x^2-1})^n \\ &= (x - z + \sqrt{x^2-1} + z)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} (x - z + \sqrt{x^2-1})^i z^{n-i}\,. \end{aligned} \tag{2.69}$$

Gegenüber dem Abschnitt 2.3.1, wo ein gemeinsamer Faktor $x-1$ herausgezogen werden konnte, stören hier die geradzahligen Potenzen von $\sqrt{x^2-1}$, aus denen zwar $x-1$ herausgezogen werden kann, nicht jedoch der Faktor $x-z$.

Multipliziert man jedoch $x - z + \sqrt{x^2-1}$ mit dem Konjugierten $x - z - \sqrt{x^2-1}$, so entsteht dadurch die Norm

$$(x - z + \sqrt{x^2-1})(x - z - \sqrt{x^2-1}) = (x-z)^2 - x^2 + 1 = -(2xz - z^2 - 1)\,, \tag{2.70}$$

also ein Element aus $\mathbb{Z}$. Deshalb multiplizieren wir beide Seiten von (2.69) einfach mit $x - z - \sqrt{x^2-1}$.

Dies liefert auf der linken Seite:

$$\begin{aligned} (x - z - \sqrt{x^2-1})(Y_1(x,n) + \sqrt{x^2-1}Y_2(x,n)) = \\ ((x-z)Y_1(x,n) - (x^2-1)Y_2(x,n)) \\ +((x-z)Y_2(x,n) - Y_1(x,n))\sqrt{x^2-1}\,. \end{aligned} \tag{2.71}$$

Auf der rechten Seite von (2.69) ergibt sich nach Abtrennung des ersten Summanden und Verwendung von (2.70):

$$
\begin{aligned}
&(x-z-\sqrt{x^2-1})\sum_{i=0}^{n}\binom{n}{i}(x-z+\sqrt{x^2-1})^i z^{n-i}\\
&\quad = (x-z-\sqrt{x^2-1})z^n\\
&\qquad + \sum_{i=1}^{n}\binom{n}{i}(x-z-\sqrt{x^2-1})(x-z+\sqrt{x^2-1})(x-z+\sqrt{x^2-1})^{i-1}z^{n-i}\\
&\quad = (x-z-\sqrt{x^2-1})z^n\\
&\qquad - (2xz-z^2-1)\sum_{i=1}^{n}\binom{n}{i}(x-z+\sqrt{x^2-1})^{i-1}z^{n-i}\,. \qquad (2.72)
\end{aligned}
$$

Gleichung (2.69) zusammen mit (2.71) und (2.72) ergibt, komponentenweise geschrieben (d. h. in$\mathbb{Z}^2$), in der zweiten Komponente

$$(x-z)Y_2(x,n) - Y_1(x,n) \equiv -z^n \pmod{2xz-z^2-1}\,. \qquad (2.73)$$

Das ist eine Gleichung, die die Funktionen Y_1 und Y_2 mit der Exponentialfunktion verbindet. Damit können wir nun analog zu (2.68) für $z,n \in \mathbb{N}_0$ und $z \geq 1$ schreiben:

$$y = z^n \Longleftrightarrow \exists x \in \mathbb{N}_0 : \begin{cases} & x > 2Y_2(z+1,n+1) \\ \wedge & y = \mathrm{rem}(Y_1(x,n)-(x-z)Y_2(x,n), 2xz-z^2-1)\,. \end{cases} \qquad (2.74)$$

Beweis :

„⇒“: Setze $x := 2Y_2(z+1,n+1)+1$. Dann gilt die erste Gleichung der rechten Seite. Weiter gilt mittels der Additionstheoreme und Bemerkung 2.1.10 $x > 2Y_2(z+1,n+1) \geq 2Y_1(z+1,n) \geq z^n$ und damit auch $2xz-z^2-1 > z^n$. Zusammen mit der aus (2.73) folgenden Gleichung $z^n \equiv \mathrm{rem}(Y_1(x,n)-(x-z)Y_2(x,n), 2xz-z^2-1)$ ergibt sich die zweite Gleichung auf der rechten Seite.

„⇐“: Wegen $x > Y_2(z+1,n+1)$ folgt entsprechend der eben gezeigten Implikation $2xz-z^2-1 > z^n$. Wegen (2.73) folgt dann $z^n = \mathrm{rem}(Y_1(x,n)-(x-z)Y_2(x,n), 2xz-z^2-1)$, also $y = z^n$.

□

Daraus ergibt sich mittels $z := x+1$ direkt folgendes Korollar:

Korollar 2.4.1 *Die Funktion $(x,n) \mapsto (x+1)^n$ ist diophantisch.*

Daraus folgt sich der wichtige Satz:

Satz 2.4.2 *Die Exponentialfunktion $(x,n) \mapsto x^n$ ist diophantisch.*

Beweis :

Es gilt

$$y = x^n \iff \begin{cases} & (x=0 \wedge y=0) \\ \vee & y = ((x-1)+1)^n\,. \end{cases}$$

□

2.5 Diophantische Gleichungen für die Binomialkoeffizienten und andere Funktionen

Wir haben unsere Hauptarbeit geleistet: Wir haben gezeigt, daß die Exponentialfunktion diophantisch ist. Für die Anwendung dieser Tatsache im Zehnten Hilbertschen Problem benötigt man weiterhin Binomialkoeffizienten und eine weitere Relation, die sich aber, wie sich sofort herausstellen wird, auf die Exponentialfunktion zurückführen lassen.

2.5.1 Die Binomialkoeffizienten

Wir schreiben entsprechend Abschnitt 2.2.1

$$x^n = (x-1+1)^n = \sum_{i=0}^{n} \binom{n}{i} (x-1)^i \,. \tag{2.75}$$

Sei nun $x > 2^n$. Es ist $\sum_{i=0}^{n} \binom{n}{i} = 2^n$, also für alle $0 \leq i \leq n$: $\binom{n}{i} < 2^n$. Also gilt $\sum_{i=0}^{j-1} \binom{n}{j} (x-1)^i < (x-1)^{j-1} 2^n < (x-1)^j$, damit gilt:

$$\operatorname{quo}(x^n, (x-1)^j) = \sum_{i=0}^{n-j} \binom{n}{i+j} (x-1)^i$$

und weiter modulo $x-1$

$$\operatorname{quo}(x^n, (x-1)^j) \equiv \binom{n}{j} \pmod{x-1}\,,$$

und wegen $\binom{n}{j} \leq 2^n < x$ gilt schließlich

$$\operatorname{rem}(\operatorname{quo}(x^n, (x-1)^j), x-1) = \binom{n}{j}\,.$$

Also können wir schreiben:

$$y = \binom{n}{j} \iff \exists x \in I\!N : x > 2^n \wedge y = \operatorname{rem}(\operatorname{quo}(x^n, (x-1)^j), x-1)\,.$$

Auf der rechten Seite stehen diophantische Funktionen bzw. Relationen, also ist die Funktion $\binom{n}{j}$ diophantisch.

2.5.2 Die Relation $\preceq$ (Bitmaskenrelation)

Definition 2.5.1 *Seien $y, x \in I\!N_0$ und sei $y = \sum_{i=0}^{n} y_i 2^i$, $x = \sum_{i=0}^{n} x_i 2^i$, mit $\forall 0 \leq i \leq n$: $x_i, y_i \in \{0,1\}$, d. h. $y_n y_{n-1} \dots y_0$ und $x_n x_{n-1} \dots x_0$ ist die duale Darstellung von y bzw. x, dann wird die Relation $\preceq$ auf $I\!N_0^2$ definiert durch*

$$x \preceq y \iff (\forall 0 \leq i \leq n : x_i \leq y_i)\,. \tag{2.76}$$

Diese Relation wird sich als sehr wichtig für das Kapitel 3 herausstellen. Deshalb wollen wir hier zeigen, daß $\preceq$ diophantisch ist.

Dies wird möglich durch die folgende Beziehung:

Lemma 2.5.2

$$x :\preceq y \Longleftrightarrow \binom{y}{x} \equiv 1 \pmod 2 . \tag{2.77}$$

Beweis :

Wir ziehen hier gegenüber dem Beweis dieses Lemmas in [1] einen etwas direkteren, aber weniger eleganteren Beweis vor.

Wir definieren zunächst die Funktion $t : I\!N \longrightarrow I\!N$ durch

$$t(y) := \max\{n \in I\!N : 2^n | y\} , \tag{2.78}$$

d. h. $t(y)$ ist die Anzahl von 2 in der Primzahlzerlegung von y.

Dann gilt $t(yy') = t(y) + t(y')$, und für $y'|y$ gilt $t(y/y') = t(y) - t(y')$, und weiter gilt

$$y \equiv 0 \pmod 2 \Longleftrightarrow t(y) > 0 . \tag{2.79}$$

Wir wenden dies nun auf Fakultäten an:

$$\begin{aligned} t(y!) &= \sum_{i=1}^{y} t(i) \\ &= \sum_{i \in \{2,\ldots,y\}, i \text{ ger.}} t(i) \\ &= \sum_{i=1}^{\lfloor y \rfloor} t(2i) \\ &= \lfloor y/2 \rfloor + \sum_{i=1}^{\lfloor y/2 \rfloor} t(i) \\ &= \lfloor y/2 \rfloor + t(\lfloor y/2 \rfloor) . \end{aligned}$$

Damit gilt

$$\begin{aligned} t\left(\binom{y}{x}\right) &= t(y!) - t((y-x)!) - t(x!) \\ &= \quad \lfloor y/2 \rfloor - \lfloor (y-x)/2 \rfloor - \lfloor x/2 \rfloor \\ &\quad + t((\lfloor y/2 \rfloor)!) - t((\lfloor (y-x)/2 \rfloor)!) - t((\lfloor x/2 \rfloor)!) . \end{aligned} \tag{2.80}$$

Ist y ungerade oder y, x gerade, dann gilt $\lfloor y/2 \rfloor = \lfloor (y-x)/2 \rfloor - \lfloor x/2 \rfloor$, und man erhält auf der rechten Seite von (2.80) einfach $t\left(\binom{\lfloor y/2 \rfloor}{\lfloor x/2 \rfloor}\right)$.

Ist y gerade und x ungerade, so erhält man auf der rechten Seite von (2.80) eine Zahl größer Null, also ist $\binom{y}{x} \equiv 0 \pmod 2$.

Also erhält man durch Induktion: $\binom{y}{x} \equiv 0 \pmod 2$ genau dann, wenn für die Ziffern x_i, y_i in der dualen Darstellung von y, x gilt $\forall i : x_i \leq y_i$. $\Box$

Bemerkung 2.5.3 *Der in [1] dargestellte Beweis fundiert auf einer allgemeineren Beziehung, die wir hier zur Ergänzung ohne Beweis angeben wollen. Sind $(x_m x_{m-1} \ldots x_0)$ und $(y_m y_{m-1} \ldots y_0)$ p-adische (p prim) Darstellungen von x, y, so gilt*

$$\binom{y}{x} \equiv \binom{y_m}{x_m}\binom{y_{m-1}}{x_{m-1}}\cdots\binom{y_0}{x_0}\,. \tag{2.81}$$

Wendet man dies auf $p = 2$ an, so erhält man die gesuchte Beziehung.

Satz 2.5.4 *Die Relation „$\preceq$" ist diophantisch.*

Beweis :

Auf der rechten Seite der Gleichung (2.77) steht eine diophantische Gleichung, damit ist „$\preceq$" diophantisch. $\square$

Kapitel 3

Die Registermaschine und ihre arithmetische Darstellung

Zur Herstellung einer Verbindung zwischen Berechenbarkeit und diophantischen Gleichungen haben wir die Wahl zwischen mehreren äquivalenten Beschreibungen der Berechenbarkeit. Wir wählen die Beschreibung, die Matijasevič in dem dieser Arbeit zugrunde liegenden Artikel [1] verwendet hat: den Begriff der Registermaschine. Von der dort gegebenen Darstellung wird etwas abgewichen.

Die Darstellung ist nicht exakt, da bei einem solchen Vorgehen die Beweisidee hinter den Formulierungen zurücktreten würde; wir sind hier aber vor allem an einer möglichst durchschaubaren Darstellung interessiert.

3.1 Die Registermaschine

Eine Registermaschine M besteht aus:

(i) Einer endlichen Zahl von Registern $\mathrm{REG}_1, \ldots, \mathrm{REG}_r$, die jeweils eine nichtnegative ganze Zahl enthalten.

(ii) Einem Programm, das heißt einer endlichen Folge von Programmanweisungen $\mathrm{LINE}_1, \ldots,$ LINE_ℓ, wobei LINE_i für alle $1 \leq i \leq \ell$ aus einer der nachstehenden Anweisungen besteht:

$$\mathrm{LINE}_i : \begin{cases} \textbf{goto } \mathrm{LINE}_k \\ \textbf{ifgtz } \mathrm{REG}_j \textbf{ goto } \mathrm{LINE}_k \\ \textbf{inc } \mathrm{REG}_j \\ \textbf{dec } \mathrm{REG}_j \end{cases} \tag{3.1}$$

mit $1 \leq j \leq r$, $1 \leq k \leq \ell + 1$. Die Zeilennummern k bzw. Registernummern j hängen dabei von i ab, diese Abhängigkeit ist aber nicht explizit dargestellt. (**ifgtz** bedeutet „**i**f **g**reater **t**han **z**ero“.)

(iii) Einem Programmzähler COUNT, der eine Zahl $p \in \{1, \ldots, \ell + 1\}$ beinhaltet.

Wir wollen nun im weiteren die Wirkungsweise einer Registermaschine erklären.

Eine Registermaschine führt eine Berechnung durch, indem sie zunächst den Programmzähler COUNT auf 1 setzt. Dann führt sie sukzessive entsprechend der in $\mathrm{LINE}_{\mathrm{COUNT}}$ enthaltenen Anweisung folgendes aus:

(i)	**goto** LINE_k:	Setze COUNT $:= k$;
(ii)	**ifgtz** REG_j **goto** LINE_k:	Falls $\mathrm{REG}_j > 0$, dann setze COUNT $:= k$, sonst setze COUNT $:=$ COUNT $+ 1$;
(iii)	**inc** REG_j:	Setze $\mathrm{REG}_j := \mathrm{REG}_j + 1$ und COUNT $:=$ COUNT $+ 1$;
(iv)	**dec** REG_j:	Falls $\mathrm{REG}_j > 0$ setze $\mathrm{REG}_j := \mathrm{REG}_j - 1$; Setze (in jedem Fall) COUNT $:=$ COUNT $+ 1$;

und zwar solange COUNT $\leq \ell$ gilt. Man beachte, daß streng genommen zwischen den Registern und dem Programmzähler einerseits und deren Inhalt andererseits unterschieden werden müßte, dies wird hier aber vernachlässigt.

Eine Registermaschine berechnet die Funktion $f : \mathbb{N}^m \longrightarrow \mathbb{N}^n$, mit $m, n \leq r$, falls sie beginnend mit $\mathrm{REG}_1 = x_1, \ldots, \mathrm{REG}_m = x_m, \mathrm{REG}_{m+1} = 0, \ldots, \mathrm{REG}_r = 0$ nach einer endlichen Anzahl von Schritten stoppt (d. h. COUNT $= \ell + 1$) und $\mathrm{REG}_1 = f_1(x_1, \ldots, x_m), \ldots, \mathrm{REG}_n = f_n(x_1, \ldots, x_m)$. Nicht genannte Register dürfen beliebige nichtnegativen Zahlen beinhalten.[1]

Die Anweisung **dec** wirkt in (iii) nicht entsprechend der Anweisung **inc**. Der Grund ist, daß verlangt wird, daß die Register nichtnegative ganze Zahlen enthalten. Ist nun aber ein Programm gegeben, so können wir jede **dec**–Anweisung durch drei Anweisungen ersetzen:

$$\mathrm{LINE}_i : \textbf{dec}\ \mathrm{REG}_j \quad \longrightarrow \begin{cases} \mathrm{LINE}_i & : \textbf{ifgtz}\ \mathrm{REG}_j\ \textbf{goto}\ \mathrm{LINE}_{i+2} \\ \mathrm{LINE}_{i+1} & : \textbf{goto}\ \mathrm{LINE}_{i+3} \\ \mathrm{LINE}_{i+2} & : \textbf{dec}\ \mathrm{REG}_j \end{cases}$$

Die anderen Sprunganweisungen müssen natürlich auch angepaßt werden. Nun kann der Befehl **dec** nicht mehr auf ein eine Null enthaltendes Register treffen. Wir können deshalb allgemein Programme voraussetzen, bei denen diese Ersetzung vorgenommen wurde, und können damit von einer einfacheren Umsetzungstabelle ausgehen:

(i)	**goto** LINE_k:	Setze COUNT $:= k$;
(ii)	**ifgtz** REG_j **goto** LINE_k:	Falls $\mathrm{REG}_j > 0$, dann setze COUNT $:= k$, sonst setze COUNT $:=$ COUNT $+ 1$;
(iii)	**inc** REG_j:	Setze $\mathrm{REG}_j := \mathrm{REG}_j + 1$ und COUNT $:=$ COUNT $+ 1$;
(iv)	**dec** REG_j:	Setze $\mathrm{REG}_j := \mathrm{REG}_j - 1$ und COUNT $:=$ COUNT $+ 1$.

Eine weitere Annahme wird später benötigt werden, nämlich, daß für alle Zeilen LINE_i : **ifgtz** REG_j **goto** LINE_k gilt, daß $k \neq i + 1$. Dies schränkt die Programme keineswegs ein, denn man sieht sofort, daß eine solche Zeile mit $k = i + 1$ einem **goto** LINE_{i+1} entspricht und damit durch einen solchen Befehl ersetzt werden kann. (Bei Korrektur der Sprunganweisungen im ganzen Programm kann die Zeile sogar weggelassen werden.)

Gegenüber dem Originalbeweis in [1] wurde hier ein Programmsprung unter der Bedingung $\mathrm{REG}_j = 0$ nicht zugelassen. Dies ist aber keine einschränkende Bedingung, da eine solche bedingte Sprunganweisung leicht mittels der folgenden beiden Zeilen erreicht werden kann:

$$\begin{aligned} \mathrm{LINE}_i &: \textbf{ifgtz}\ \mathrm{REG}_j\ \textbf{goto}\ \mathrm{LINE}_{i+2} \\ \mathrm{LINE}_{i+1} &: \textbf{goto}\ \mathrm{LINE}_k \end{aligned}$$

[1] Die Forderung $\mathrm{REG}_{m+1} = 0, \ldots, \mathrm{REG}_r = 0$ wird nur für unseren Zweck in den nächsten Abschnitten benötigt. Es ist klar, daß man durch Veränderung des Programms dafür sorgen kann, daß die Maschine auch ohne diese Forderung eine Berechnung korrekt durchführt.

Man beachte, daß während einer Programmbearbeitung die Inhalte von $\mathrm{REG}_1, \ldots, \mathrm{REG}_r$, COUNT veränderlich sind und auch vom Input x abhängen. Die Inhalte von $\mathrm{LINE}_1, \ldots, \mathrm{LINE}_\ell$ hängen aber nur von der zu berechnenden Funktion ab.

Wie bereits erwähnt ist die Registermaschine eine der möglichen Beschreibungsmöglichkeiten für berechenbare Funktionen. Dies wird im folgenden Satz formuliert, ohne den Beweis anzugeben (entsprechend den Grundlagen aus Abschnitt 1.2.)

Satz 3.1.1 *Eine Funktion $f : \mathbb{N}^n \to \mathbb{N}^m$ ist genau dann berechenbar (d. h. $\in B_{n,m}$), wenn eine Registermaschine existiert, die f berechnet.*

3.2 Die arithmetische Darstellung einer Berechnung

Unser Ziel ist es, die Äquivalenz zwischen der Diophantizität und der Berechenbarkeit einer Funktion zu zeigen. Die eine Richtung ist einfach und schon in Kapitel 1 gezeigt. Wesentlich ist es, die Berechenbarkeit einer Funktion durch diophantische Funktionen darzustellen.

Das Lemma 1.4.3 liefert die Diophantizität des Schnittes bzw. der Vereinigung einer festen Anzahl diophantischer Mengen. Da aber die Länge der Berechnung einer Funktion i. a. vom Input abhängt, muß man versuchen, den ganzen Verlauf einer Berechnung in einer festen Anzahl von Zahlen zu kodieren. Dieses Problem taucht auch bei Verwendung anderer Definitionen für Berechenbarkeit auf, was wir hier aber nicht weiter ausführen wollen. Diese Kodierung wird bei den Registermaschinen nun dadurch bewerkstelligt, daß man die während der Berechnung auftretenden Inhalte der Register als Stellen der Q–adischen Darstellung einer Zahl kodiert, wobei Q vom Input abhängt und größer sein muß als die während der Berechnung in den Registern enthaltenen Zahlen.

Hierin liegt nun der Vorteil der Registermaschine begründet: da die Register in einem Schritt höchstens inkrementiert werden können, ist der maximale Registerinhalt durch die Summe des maximalen Inputs und der Berechnungslänge beschränkt.[2] Das macht die Wahl von Q entsprechend leicht.

Wir wollen also nun im folgenden eine Berechnung in einen Satz von Zahlen kodieren. Dabei gehen wir zunächst von einer Funktion $f : \mathbb{N} \longrightarrow \mathbb{N}$ aus, was hier die Beschreibung etwas vereinfacht.

Die Berechnung einer Registermaschine läuft schrittweise. Wir führen deshalb die Variable t ein, die die Anzahl der absolvierten Schritte bezeichnet. Wir bezeichnen mit $r_{j,t}$ den Inhalt von REG_j nach t Schritten. $r_{j,0}$ ist der Inhalt von REG_j bei Beginn der Berechnung.

Gehen wir von der Berechnung eines $y = f(x)$ aus, die in s Schritten absolviert wird, so gilt $r_{1,0} = x$ und $r_{1,s} = y$.

Beachtet man, daß bei jedem Berechnungsschritt ein Register nur um eins erhöht werden kann, so folgt für alle $0 \le t \le s$ die Ungleichung $r_{1,t} \le x + t$ und für alle $0 \le t \le s$ und $2 \le i \le r$ die Ungleichung $r_{i,t} \le t$.

Wir definieren nun

$$Q := 2^{x+s+\ell+2} . \tag{3.2}$$

Damit erfüllt Q die folgenden Bedingungen:

$$Q \quad > \quad 4(x+s) , \tag{3.3}$$

[2] Deswegen wurde der Inhalt 0 der Nicht–Input–Register zu Beginn der Berechnung verlangt.

$$\begin{aligned} Q &> \ell+1\,, &(3.4)\\ \exists n \in I\!N:\ Q &= 2^n\,. &(3.5)\end{aligned}$$

Also gilt für alle $1 \leq i \leq r$, $0 \leq t \leq s$ die Gleichung $r_{j,t} < Q/4$.[3]

Sei $R_1, \ldots, R_r$ durch

$$R_j := \sum_{t=0}^{s} r_{j,t} Q^t \tag{3.6}$$

definiert. Dann gilt aufgrund von $Q > 2r_{j,t} \geq r_{j,t}$, daß in R_j die Registerinhalte $r_{j,0}, \ldots, r_{j,s}$ kodiert sind. Wenn wir im folgenden von der Q^t-er Stelle einer Zahl sprechen, so ist damit die $(t+1)$-te Stelle von rechts in der Q-adischen Darstellung dieser Zahl gemeint, was z. B. bei R_j mit $r_{j,t}$ identisch ist. Wir benötigen diese Bezeichnung bei zusammengesetzten Ausdrücken.

$R_1, \ldots, R_r$ kodieren also die Register während der Berechnung. Nun wollen wir auch die Inhalte von COUNT kodieren.

$$\forall \quad 1 \leq j \leq \ell+1, \quad 0 \leq t \leq s: \quad \ell_{j,t} := \begin{cases} 1 \text{ falls COUNT} = j \text{ zur Zeit } t \\ 0 \text{ sonst}\,. \end{cases} \tag{3.7}$$

und entsprechend der Definition von den R_j wird nun L_j durch

$$\forall 1 \leq j \leq \ell+1: \quad L_j := \sum_{t=0}^{s} \ell_{j,t} Q^t \tag{3.8}$$

definiert. Da der Inhalt von COUNT auch $\ell+1$ sein kann (Haltebedingung), muß entsprechend auch $L_{\ell+1}$ definiert werden.

Wir definieren nun noch I durch

$$I := \sum_{t=0}^{s} Q^t = \frac{Q^{s+1}-1}{Q-1}\,, \tag{3.9}$$

d. h. die Q^t-er Stelle von I ist immer 1.

3.3 Die Kodierung des Programms

Wir haben nun die Berechnung der Registermaschine durch die Zahlen $R_1, \ldots, R_r, L_1, \ldots, L_{\ell+1}$ ausgedrückt. Die Steuerung der Berechnung erfolgt durch das Programm; dies kann arithmetisch durch Bedingungen an die Größen $R_1, \ldots, R_r, L_1, \ldots, L_{\ell+1}$ ausgedrückt werden.

All diese Bedingungen zusammen müssen äquivalent zur Berechnung durch die Registermaschinen sein, d. h. die Registermaschine berechnet die Funktion f genau dann, wenn diese Bedingungen erfüllt sind. Wir gehen dabei so vor, daß wir aus der Sicht der Berechenbarkeit von f notwendige Bedingungen an $R_1, \ldots, R_r, L_1, \ldots, L_{\ell+1}$ ausdrücken werden. Am Ende muß dann noch gezeigt werden, daß diese Bedingungen auch hinreichend sind.

Zunächst drücken wir die Tatsache aus, daß die Maschine immer genau eine Zeile bearbeitet, bei Zeile 1 beginnt und bei Sprung auf $\ell+1$ stoppt. Dies kann recht einfach in den entsprechenden Zahlen ausgedrückt werden.

Die Bedingung

$$\forall 1 \leq i \leq \ell: L_i \preceq I \tag{3.10}$$

[3] Gegenüber der Vorlage wurde der dort verwendete Faktor 2 hier durch 4 ersetzt; das vereinfacht die Interpretation von (3.17).

drückt die Tatsache aus, daß L_i entsprechend der Definition an jeder Stelle der Q–adischen Darstellung höchstens eine 1 besitzt.

Die Bedingung
$$\forall 1 \leq j \leq r : R_j \preceq (Q/4 - 1)I \tag{3.11}$$
drückt aus, daß die $r_{j,t}$ alle kleiner sind als $Q/4$. Tatsächlich ist Q gerade so gewählt worden.

Die Bedingung
$$\sum_{i=1}^{\ell+1} L_i \preceq I \tag{3.12}$$
drückt aus, daß zu jeder Zeit genau eine Programmzeile abgearbeitet wird. Denn durch Betrachtung aller Stellen in dieser Bedingung folgt: (3.12) $\iff \forall 0 \leq t \leq s : \sum_{i=1}^{\ell} \ell_{i,t} \leq 1 \iff \forall 0 \leq t \leq s : \quad \exists_1 i : \ell_{i,t} = 1$, was bedeutet, daß jeweils immer genau eine Zeile bearbeitet wird.

Die Bedingung
$$1 \preceq L_1 \tag{3.13}$$
ist äquivalent zu $\ell_{1,0} \geq 1$, was zusammen mit den schon aufgeführten Bedingungen äquivalent ist zu $\ell_{1,0} = 1$ und bedeutet, daß bei $t = 0$ mit der ersten Zeile begonnen wird.
$$Q^s = L_{\ell+1} \tag{3.14}$$
ist äquivalent zu $\forall 0 \leq t < s : \quad \ell_{\ell+1,t} = 0$ und $\ell_{\ell+1,s} = 1$. Dies bedeutet, daß erst im letzten Schritt COUNT $= \ell + 1$ wird.

Nun werden die einzelnen Anweisungen ausgedrückt, wobei jeweils davon ausgegangen wird, daß die jeweils angeführte Anweisung in Zeile LINE$_i$ steht.

goto LINE$_k$: Die Bedingung
$$QL_i \preceq L_k \tag{3.15}$$
ist äquivalent zu: $\forall 0 \leq t \leq s - 1 : \ell_{i,t} \leq \ell_{k,t+1}$. Dies bedeutet, daß jedesmal, wenn die i-te Zeile abgearbeitet wird, der Programmzähler auf k gesetzt wird, was einem LINE$_i$: **goto** LINE$_k$ entspricht.

ifgtz REG$_j$ **goto** LINE$_k$: Die Anweisung LINE$_i$: **ifgtz** REG$_j$ **goto** LINE$_k$ beinhaltet eine Entscheidung. Zunächst wird durch die Bedingung
$$QL_i \preceq L_{i+1} + L_k \tag{3.16}$$
ausgedrückt, daß nach dem Ausführen der i-ten Zeile entweder der Programmzähler auf $i + 1$ oder k gesetzt wird. Man beachte, daß $k \neq i + 1$ vorausgesetzt wurde.

Die Bedingung
$$QL_i \preceq L_k + QI - 4R_j \tag{3.17}$$
ist etwas schwieriger einzusehen. Zunächst sieht man sofort, daß aufgrund der Beschränkung von $r_{j,t}$ beim Ausdruck auf der rechten Seite höchstens von einer Stelle in der Q–er Darstellung zur anderen ein Übertrag von -1 entstehen kann. Dies geschieht aber nur dann, wenn an der entsprechenden Stelle $r_{j,t} > 0$ ist.

Die Q^{t+1}-er Stelle der linken Seite ist $\ell_{i,t}$. Falls $r_{j,t} = 0$, so steht (modulo Q) an der Q^{t+1}-er Stelle der rechten Seite von (3.17) $\ell_{k,t+1} + 1 - 2r_{j,t+1}$, was die umgekehrte Parität (d. h. gerade/ungerade) zu $\ell_{k,t+1}$ hat. Ist nun $\ell_{i,t} = 1$, so muß zur Erfüllung von (3.17) $\ell_{k,t+1}+1-2r_{j,t+1}$ ungerade, d. h. $\ell_{k,t+1} = 0$, und damit $\ell_{i+1,t+1} = 1$ sein, d. h. die nächste Zeile wird ausgeführt.

Ist umgekehrt $r_{j,t} > 0$, so ergibt sich an der Q^t–er Stelle ein Übertrag von -1 an die Q^{t+1}–er Stelle. Zusammen mit der 1 von QI verbleibt dann an der Q^{t+1}–er Stelle nur noch $\ell_{k,t+1} - 4r_{j,t+1}$. Ist nun $\ell_{j,t} = 1$, so muß zur Erfüllung der Forderung $\ell_{k,t+1} = 1$ sein, d. h. das Programm fährt mit der k–ten Zeile fort. Damit entspricht die dargestellte Formel einer Anweisung LINE_i : **ifgtz** REG_j **goto** LINE_k.

inc/dec REG_j**:** Die Bedingung

$$QL_i \preceq L_{i+1} \tag{3.18}$$

drückt aus, daß nach Inkrementierung/Dekrementierung die Bearbeitung bei der nächsten Zeile weitergeht.

Sodann definieren wir die (nur vom Programm, nicht vom Input x abhängigen) Mengen

$$\begin{aligned} K_j^+ &:= \{i|\mathrm{LINE}_i \text{ enthält Anweisung INC } \mathrm{REG}_j\}, \\ K_j^- &:= \{i|\mathrm{LINE}_i \text{ enthält Anweisung DEC } \mathrm{REG}_j\}. \end{aligned}$$

Dann drücken

$$R_1 + yQ^{s+1} = x + QR_1 + \sum_{i \in K_1^+} QL_i - \sum_{i \in K_1^-} QL_i \tag{3.19}$$

und

$$\forall \quad j = 2, \dots, r: \quad R_j = QR_j + \sum_{i \in K_j^+} QL_i - \sum_{i \in K_j^-} QL_i \tag{3.20}$$

die Wirkung der Dekrement/Inkrement–Befehle aus. Denn die Q^{t+1}-er Stelle von der rechten Seite von 3.20 ist $r_{j,t}$, falls im t-ten Schritt der Programmzähler auf keinem **inc/dec**-Befehl steht, oder $r_{j,t} \pm 1$, falls der Programmzähler auf einer einen solchen Befehl beinhaltenden Zeile steht.

Nun müssen wir überlegen, ob die Bedingungen (3.2), (3.9), (3.10)–(3.20) (wovon einige aus mehreren einzelnen Bedingungen bestehen) hinreichend dafür sind, daß die betrachtete Registermaschine $f(x)$ berechnet. Dies formal darzustellen wäre zu kompliziert, wir führen deshalb keinen formalen Beweis, sondern eher eine Begründung.

Die Bedingungen (3.2) und (3.9) definieren die Zahlen Q und I, die wesentlich für die richtige Interpretation der anderen Bedingungen sind. Die Gleichungen (3.10), (3.12), (3.13) und (3.14) sagen uns, daß aus den $L_1, \dots, L_\ell$ die Abfolge von Programmschritten nachvollzogen werden kann, die Programmbearbeitung mit COUNT $= 1$ beginnt und irgendwann mit COUNT $= \ell + 1$ stoppt. Aus (3.11) erhält man die Bedingung, daß (3.17) richtig interpretiert werden kann. Da wir nun den Verlauf der Berechnung kennen, sagen uns die Bedingungen (3.15)–(3.20), daß die Zahlen COUNT, $\mathrm{REG}_1, \dots, \mathrm{REG}_r$ genau den Änderungen unterworfen sind, die eine Registermaschine bewirken würde. Schließlich ergibt (3.20) noch, daß der Input x und der Output $f(x) = y$ ist.

Damit sind die Bedingungen (3.2), (3.9), (3.10)–(3.20) äquivalent dazu, daß eine Registermaschine $f(x)$ berechnet. Das heißt, die Registermaschine berechnet f genau dann, wenn $\exists Q, I, L_1, \dots, L_{\ell+1}, R_1, \dots, R_r \in \mathbb{N}_0$ mit (3.2), (3.9), (3.10)–(3.20).

Nun sind die Bedingungen (3.2), (3.9), (3.10)–(3.20) alle diophantisch. Also folgt aus $f : \mathbb{N}_0 \to \mathbb{N}_0$ berechenbar mittels einer Registermaschine, daß f diophantisch ist, und mittels Satz 3.1.1 ergibt sich, daß alle berechenbaren Funktionen aus $B_{n,1}$ diophantisch sind.

Die Bedingung (3.19) ist die einzige, die eine Änderung bei einer Berechnung einer Funktion $f : \mathbb{N}^m \Rightarrow \mathbb{N}^n$ erfordert. Für $j = 1, \dots, m$ ist auf der rechten Seite der Gleichung für R_j ein x_j einzufügen, und für $j = 1, \dots, n$ ist auf der linken Seite der Gleichung für R_j ein $y_j Q^{s+1}$

einzufügen. Damit können wir ganz entsprechend sagen, daß aus $f \in B_{m,n}$ die Diophantizität von f folgt. Wir geben das noch in einem Korollar an:

Korollar 3.3.1 *Für $f : I\!N_0^m \to I\!N_0^n$ gilt*

$$f \text{ berechenbar} \quad \Longrightarrow \quad f \text{ diophantisch}. \tag{3.21}$$

Wir haben nun die schwierige Implikation des Satzes 1.3.3 gezeigt, so daß dieser Satz vollständig bewiesen ist. Damit ist auch Satz 1.3.1 gezeigt, woraus dann die Lösung des Zehnten Hilbertschen Problems abgeleitet wurde. Somit haben wir nun unser Ziel erreicht.

Für die Diophantizität von 3.2 und 3.9 war es nötig, die Exponentialfunktion diophantisch darzustellen. Weiterhin wurde die diophantische Gleichung der Exponentialfunktion bei der Darstellung der Relation $\preceq$ als diophantische Relation benötigt.

Zusammenfassung

Wir wollen hier diese Arbeit noch einmal zusammenfassen. Mit dem der Arbeit zugrunde liegenden Artikel von Matijasevič [1] wurde ein in den einzelnen Schritten leicht nachvollziehbarer Beweis für die Unlösbarkeit (im Sinne der Churchen These) des Zehnten Hilbertschen Problems vorgestellt. Damit kann man sich beruhigt zurücklehnen und braucht keine Anstrengung mehr zu unternehmen, ein Computerprogramm zu entwickeln, das entscheidet, ob eine diophantische Gleichung lösbar ist oder nicht.

Allerdings kommt einem bei der Durchsicht des Artikels die Frage, wie jemandem solche Kongruenzen für die Lösungen der Pellschen Gleichungen in den Sinn kommen. Ersichtlich ist nur, daß zum Beweis des wesentlichen Satzes, nämlich daß die Funktionen Y_1 und Y_2 diophantisch sind, viele Eigenheiten dieser Lösungen ausgenützt werden.

In dieser Arbeit wurde versucht, diese Eigenheiten zu motivieren, indem man anhand der Potenzen ganzer Zahlen eine Beweisparallele erzeugt, die zwar für den Beweis nicht notwendig ist, aber die Probleme des Beweises aufzeigt, ohne mit den uneinsichtigen Lösungen der Pellschen Gleichung zu arbeiten. Damit sind die eigentlichen Probleme sichtbarer.

Wenn man dann die gewonnene Methode auf die Lösungen der Pellschen Gleichung überträgt, so ergeben sich die in [1] wenig motivierten Kongruenzen mehr oder weniger leicht aus dieser Übertragung.

Weiterhin zeigt die Beweisparalelle auch klar, daß die anscheinend sehr speziellen Eigenschaften der Lösungen der Pellschen Gleichung so speziell gar nicht sind, sondern daß die für den Beweis benötigten wesentlichen Eigenschaften in anderer Form auch bei anderen Folgen zu finden sind.

Anhang A

A.1 Alternative Definitionen diophantischer Mengen

Wie im ersten Kapitel erwähnt, besteht in der Definition einer diophantischen Menge eine gewisse Willkür. Zur Untersuchung dieses Umstandes betonen wir zunächst, daß in unserer Definition drei Kategorien von Zahlen auftreten: die Parameter, die Lösungen und die Polynomkoeffizienten.

Hilbert[4] hatte das Problem ohne Hinzunahme von Parametern sinngemäß so formuliert: Gesucht ist ein Algorithmus, der bei einem gegebenen Polynom mit ganzzahligen Koeffizienten in den Unbekannten $x_1, \ldots, x_m$ entscheidet, ob die Gleichung $P(x_1, \ldots, x_m) = 0$ eine ganzzahlige Lösung[1] hat.

In unserer Definition diophantischer Mengen erscheinen zusätzlich noch Parameter $(a_1, \ldots, a_n)$. Diese Parametrisierung wird nur zur Formulierung der Lösung benötigt, und hierfür ist es am einfachsten und auch ausreichend, diophantische Mengen als Teilmengen von $\mathbb{N}_0^n$ vorauszusetzen, d. h. die Parameter die nichtnegativen ganzen Zahlen durchlaufen zu lassen.

Die Suche nach ganzzahligen und nach nichtnegativen ganzen Lösungen ist äquivalent in dem Sinne, daß ein Algorithmus, der das eine Problem löst, auch jeweils das andere Problem löst, wobei sich jeweils die Polynome transformieren. Wir können es auch formaler beschreiben, indem wir eine an die Definition 1.1.3 angelehnte Definition geben und dann die Äquivalenz beider Definitionen zeigen.

Definition A.1.1 *Sei $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$. Wir nennen A ganzzahlig–diophantisch genau dann, wenn ein $m \in \mathbb{N}_0$ und ein Polynom $P \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ existiert, so daß*

$$A(a_1, \ldots, a_n) \iff \exists x_1, \ldots, x_m \in \mathbb{Z} \quad \text{mit} \quad P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\,. \tag{A.1}$$

Diese Defintion unterscheidet sich von Definition 1.1.3 nur durch die Menge, aus der die $x_1, \ldots, x_m$ stammen.

Satz A.1.2 *Sei $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$. Dann ist A diophantisch genau dann, wenn A ganzzahlig–diophantisch ist.*

Beweis :

„$\Rightarrow$“: Da jede nichtnegative ganze Zahl sich als Summe von Quadraten von vier ganzen Zahlen darstellen läßt — sei für $i = 1, \ldots, m$ insbesondere $x_i = x_{i1}^2 + x_{i2}^2 + x_{i3}^2 + x_{i4}^2$ —, können

[1] Eine Lösung mit ganzzahligen $x_1, \ldots, x_m$; diese abkürzende Formulierung wird im folgenden häufiger verwendet.

wir schreiben

$$\begin{aligned} A(a_1,\dots,a_n) &\iff \exists x_1,\dots,x_m \in \mathbb{N}_0 \ \text{ mit } \ P(a_1,\dots,a_n,x_1,\dots,x_m)=0 \\ &\iff \exists x_{11},\dots,x_{m4} \in \mathbb{Z} \ \text{ mit } \ P(a_1,\dots,a_n,\sum_{j=1}^{4} x_{1j}^2,\dots,\sum_{j=1}^{4} x_{mj}^2)=0\,, \end{aligned}$$

wobei in der letzten Zeile $P(\dots)$ als ein Polynom in den Variablen $x_{11},\dots,x_{m4}$ zu lesen ist. Die Rückrichtung der Äquivalenzen ist einfach durch $x_i := x_{i1}^2 + x_{i2}^2 + x_{i3}^2 + x_{i4}^2 \in \mathbb{N}_0$ zu erhalten.

„$\Leftarrow$“: Wir schreiben einfach

$$\begin{aligned} &A(a_1,\dots,a_n) \\ &\iff \exists x_1,\dots,x_m \in \mathbb{Z} \ \text{ mit } \ P(a_1,\dots,a_n,x_1,\dots,x_m)=0 \\ &\iff \exists x_1,\dots,x_m \in \mathbb{N}_0, \epsilon_1,\dots,\epsilon_m \in \{\pm 1\} \ \text{ mit } \ P(a_1,\dots,a_n,\epsilon_1 x_1,\dots,\epsilon_m x_m)=0 \\ &\iff \exists x_1,\dots,x_m \in \mathbb{N}_0 \ \text{ mit } \ \prod_{\epsilon_1=\pm 1} \cdots \prod_{\epsilon_m=\pm 1} P(a_1,\dots,a_n,\epsilon_1 x_1,\dots,\epsilon_m x_m)=0\,. \end{aligned}$$

Da für $\epsilon_1,\dots,\epsilon_m$ nur eine endliche Anzahl von Möglichkeiten existiert, ist das in der letzten Zeile stehende Produkt von Polynomen wieder ein Polynom (aber nun ohne $\epsilon_1,\dots,\epsilon_m$). Da ein Produkt genau dann verschwindet, wenn einer der Faktoren verschwindet, ergibt sich die letzte Äquivalenz.

□

Es ist aber zu beachten, daß bei einem konkret gegebenen Polyonom von Bedeutung ist, ob man nach nichtnegativen oder beliebigen ganzen Lösungen sucht. Allgemeiner kann man sagen, daß wenn man in beiden Definitionen jeweils die zugelassenen Polynome einschränken würde, die Definitionen nicht mehr äquivalent sein müssen. Nur die in beiden Definitionen verwendete Wahl von $\mathbb{Z}[a_1,\dots,a_n,x_1\dots,x_m]$ als Menge der zulässigen Polynome garantiert die Äquivalenz.

Beschränkte man sich z. B. in beiden Definitionen auf Polynome mit nichtnegativen Koeffizienten, so wäre die Äquivalenz nicht mehr gegeben. Zur Darstellung dieser Tatsache definieren wir zunächst einen der entsprechenden Begriffe und zeigen die Äquivalenz mit den schon gegebenen Begriffen. Von dem anderen zeigen wir, daß er etwas Uninteressantes liefert.

Definition A.1.3 *Sei $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$. Wir nennen A $\mathbb{N}_0$–polynomial–diophantisch genau dann, wenn ein $m \in \mathbb{N}_0$ und ein Polynom $P \in \mathbb{Z}[a_1,\dots,a_n,x_1,\dots,x_m]$ mit Koeffizienten aus $\mathbb{N}_0$ existiert, so daß*

$$A(a_1,\dots,a_n) \iff \exists x_1,\dots,x_m \in \mathbb{Z} \ \textit{ mit } \ P(a_1,\dots,a_n,x_1,\dots,x_m)=0\,. \tag{A.2}$$

Dann können wir zunächst schreiben:

Satz A.1.4 *Sei $n \in \mathbb{N}$ und $A \subset \mathbb{N}_0^n$. Dann ist A diophantisch genau dann, wenn A $\mathbb{N}_0$–polynomial–diophantisch ist.*

Beweis :

Für die Richtung von rechts nach links ist nichts zu beweisen. Der Beweis der anderen Richtung ist in der Idee sehr einfach. Um diese aber nicht in reinem Formalismus untergehen zu lassen, wird hier der Beweis nicht formal voll ausgführt.

Man ersetze in jedem Monom α von P mit einem Koeffizienten $c_\alpha < 0$ den Koeffizienten durch $\epsilon_\alpha(-c_\alpha)$; dies sei P', welches nun Koeffizienten ≥ 0 hat. Dann addiere man zu dem Quadrat von P' die Summe $\sum_\alpha(\epsilon_\alpha + 1)^2$ hinzu. Dadurch erhält man ein Polyonom R mit nichtnegativen Koeffizienten und zusätzlichen Unbekannten ϵ_α.

Aus einer Lösung $x_1, \ldots, x_m$ von $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ erhält man durch Setzen aller ϵ_α auf -1 und Beibehalten aller x_i eine Lösung von $R(\ldots) = 0$.

Umgekehrt folgt für eine Lösung von $R(\ldots) = 0$ sofort $\epsilon_\alpha = -1$ für alle α; setzt man dies in P' ein, so erhält man wieder P. Die Gleichung $R(\ldots) = 0$ liefert aber gleichzeitig auch das Verschwinden von P', damit liefern die $x_1, \ldots, x_m$ eine Lösung von $P(\ldots)$. $\square$

Im entsprechenden Gegenstück zu den $I\!N_0$–polynomial–diophantischen Relationen wären sowohl die Koeffizienten des Polynoms, die Parameter und die Unbekannten aus $I\!N_0$. Damit ist $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ genau dann lösbar in $x_1, \ldots, x_m$, wenn $Q(a_1, \ldots, a_n) := P(a_1, \ldots, a_n, 0, \ldots, 0) = 0$. Hierzu muß das konstante Glied von P Null sein. Weiterhin müssen die Parameter entweder Null sein, oder sie sind beliebig (je nachdem, welche Monome in Q auftreten).

Die entsprechende Definition einer solchen Diophantizität ist uninteressant und deckt sich offensichtlich nicht mit den anderen Begriffen.

Man sieht hier, daß die Begriffe vielfältig variiert werden können. Weiterhin können wir auch den Begriff der Diophantizität aus Definition 1.1.3 darin ändern, daß wir als Unbekannte alle rationalen Zahlen zulassen. Es ist bis heute noch unbekannt, ob solchermaßen definierte diophantische Mengen entscheidbar sind.

A.2 Der Allquantor bei diophantischen Mengen

Wir wollen hier die Bemerkung 1.4.6 (i) etwas genauer ausführen. Sei $n \in I\!N$ und $A \subset I\!N_0^{n+1}$ diophantisch, dann ist die durch

$$B(a_1, \ldots, a_n) :\Longleftrightarrow \quad \forall a \in I\!N_0 : A(a, a_1, \ldots, a_n) \tag{A.3}$$

definierte Menge $B \in I\!N_0^n$ i. a. nicht diophantisch.

Unter Verwendung von Satz 1.3.1 ist nur entsprechend zu zeigen, daß mit oben definierten A, B aus der Aufzählbarkeit von A nicht die Aufzählbarkeit von B folgt.

Wir zeigen dies indirekt. Sei mit $A \in I\!N_0^{n+1}$ aufzählbar auch die mittels Gleichung (A.3) definierte Relation B aufzählbar, und sei $\{\} \neq C \subset I\!N_0$ aufzählbar. Damit existiert nach Definition ein $m \in I\!N$ und $f \in B_{m,1}$ mit $\mathrm{im}(f) = C$. Nach Satz 1.2.8 ist $\mathrm{graph}(f)$ entscheidbar und dann nach Lemma 1.2.6 $I\!N_0^{m+1} \backslash \mathrm{graph}(f)$ aufzählbar. Damit ist aber die durch $D(a) :\Longleftrightarrow \forall a_1, \ldots, a_m : (a_1, \ldots, a_m, a) \notin \mathrm{graph}(f)$ definierte Relation D aufgrund unserer Annahme auch aufzählbar. Andererseits ist $D = I\!N_0 \backslash \mathrm{im}(f) = I\!N_0 \backslash C$. Damit ist auch $I\!N_0 \backslash C$ aufzählbar und damit nach Lemma 1.2.6 C sogar entscheidbar. Da C nicht speziell war, folgt, daß jede aufzählbare Menge entscheidbar ist — im Widerspruch zu Satz 1.2.7. Damit ist die angenommene Implikation nicht allgemein (für alle n) gültig. Die nicht ausgeführte Beschränkung auf ein bestimmtes n ist nicht essentiell, was hier aber nicht weiter ausgeführt werden soll.

Literaturverzeichnis

[1] J.P. Jones, Y.V. Matijasevič; Proof of recursive unsolvability of Hilbert's tenth problem; Amer. Math. Monthly 98 (1991), no. 8, 689–709.

[2] Y.V. Matijasevič; Enumerable sets are diophantine; Doklady Akademii Nauk SSSR, 191 (1970), 279–282.

[3] M.D. Davis, H. Putnam, J. Robinson; The decision problem for exponentail diophantine equations; Annals of Math. Series 2, 74 (1961), 425–436.

[4] D. Hilbert; Mathematische Probleme, Vortrag gehalten auf dem Internationalen Mathmatiker Kongreß in Paris im Jahre 1900; Nachrichten der Akademie der Wissenschaften in Göttingen.

[5] Hermes; Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit; Springer–Verlag 1978.

[6] N. Jacobson; Basic Algebra; W.H. Freeman and Company 1985.

[7] D.A. Marcus; Number Fields; Springer–Verlag 1987.

Bezeichnungen

$\cup, \cap, \setminus$	Mengenoperationen: Vereinigung, Schnitt, Minus
$\mathbb{N}$	Die natürlichen Zahlen
$\mathbb{N}_0$	Die nichtnegativen ganzen Zahlen
$\mathbb{Z}$	Die ganzen Zahlen
$\mathbb{R}$	Die reellen Zahlen
$R^\times$	Die Einheitengruppe von R
$\forall$	Der Allquantor: Für alle ....
$\exists$	Der Existenzquantor: Es existiert ...
$\exists_1$	Es existiert genau ein ...
$\{x \in \ldots \mid \ldots\}$	Menge aller $x \in \ldots$ mit Eigenschaft $\ldots$
$x \mid y$	x teilt y
$\lceil x \rceil$	$\max\{z \in \mathbb{Z} \mid z \leq x\}$
$\lfloor x \rfloor$	$\min\{z \in \mathbb{Z} \mid z \geq x\}$
I_A	charakteristische Funktion, d. h. $I_A(x) := \begin{cases} 1 & \text{für } x \in A \\ 0 & \text{für } x \notin A \end{cases}$
$\mathrm{quo}(x, y)$	$\lceil x/y \rceil$
$\mathrm{rem}(x, y)$	$x - y\,\mathrm{quo}(x, y)$