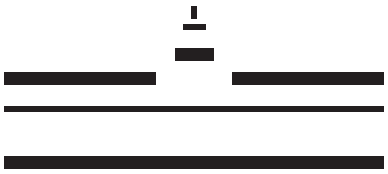

Westfälische
Wilhelms-Universität
Münster

Hilberts 10. Problem: Diophantische Mengen sind nicht entscheidbar

Bachelorarbeit
zur Erlangung des akademischen Grades
Bachelor of Science

Westfälische Wilhelms-Universität Münster
Fachbereich Mathematik und Informatik
Institut für Mathematische Logik und Grundlagenforschung

Eingereicht von:
Justin Dreyer

Betreuung:
Dr. Franziska Jahnke

Zweitgutachterin:
Prof. Dr. Dr. Katrin Tent

Münster, Juli 2016

Inhaltsverzeichnis

1 Einleitung

> „Es ist schwierig und oft unmöglich, den Wert eines Problems im Voraus richtig zu beurteilen; denn schließlich entscheidet der Gewinn, den die Wissenschaft dem Problem verdankt."
>
> David Hilbert[1]

Der deutsche Mathematiker David Hilbert, der als einer der größten Mathematiker seiner Zeit gilt, präsentierte im Jahr 1900 auf dem Internationalen Mathematiker-Kongress in Paris eine Liste der seiner Meinung nach wichtigsten offenen Probleme der Mathematik. Später veröffentliche er in [Hil00] eine Liste von 23 offenen Problemen der Mathematik, die heute als die *Hilbertschen Probleme* bekannt sind. Diese Liste hat die Entwicklung der Mathematik im 20. Jahrhundert maßgeblich beeinflusst und motiviert. Bis heute sind einige dieser Probleme ungelöst und von manchen konnte man zeigen, dass sie unbeweisbar sind (Hilberts 1. Problem: die Kontinuumshypothese[2], vgl. [Sch14, Theorem 6.33]).

Wir möchten uns mit dem 10. Problem beschäftigen, das wir kurz als *H10* bezeichnen. Die Formulierung lautet:

> „*Eine* Diophantische Gleichung *mit irgend welchen Unbekannten und mit* ganzen rationalen Zahlencoefficienten *sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer* endlichen Anzahl von Operationen *entscheiden läßt, ob die Gleichung in* ganzen rationalen Zahlen *lösbar ist*[3]." [Hil00, S. 276]

Hilbert fragt also – nach heutigem Verständnis – nach einem Algorithmus, der die Lösbarkeit diophantischer Gleichungen entscheidet und nach endlicher Zeit terminiert. Die Formulierung lässt schließen, dass er die Existenz eines solchen Algorithmus erwartete. Der Begriff *Algorithmus* wurde im Laufe des 20. Jahrhunderts formalisiert. Der Mathematiker Alan Turing[4] lieferte den Beweis für das überraschende Resultat, dass es unlösbare bzw. unentscheidbare Probleme[5] gibt (vgl. [HMU01, Kapitel 9]).

[1] David Hilbert (⋆1862, †1943) war ein deutscher Mathematiker, der ein breites Spektrum grundlegender Ideen in vielen Bereichen der Mathematik entwickelte.

[2] Die Kontinuumshypothese besagt, dass es keine Menge gibt, die in ihrer Mächtigkeit größer ist als $\mathbb{N}$ und kleiner als $\mathbb{R}$. Dieses Problem ist in ZFC nicht entscheidbar.

[3] Hervorhebungen durch den Verfasser

[4] Alan Turing (⋆1912, †1954) war ein britischer Mathematiker, der mit seinen Arbeiten die Grundlagen für die Informatik lieferte.

[5] Das Halteproblem bezeichnet die Frage, ob ein gegebener Algorithmus (oder eine Turingmaschine) für eine gegebene Eingabe terminiert, also nach endlich vielen Schritten anhält. Turing konnte beweisen, dass es keinen Algorithmus gibt, der das Halteproblem für alle möglichen Algorithmen und Eingaben entscheiden kann.

Frühere Arbeiten von Martin Davis[6], Hilary Putnam[7] und Julia Robinson[8] ergaben, dass die negative Lösung von H10 folgt, sobald eine diophantische Definition der Exponentialfunktion gefunden wird. Der russische Mathematiker Yuri Matijasevič[9] lieferte diese im Jahr 1970 im Alter von 22 Jahren mithilfe der Fibonacci-Zahlen.

In der vorliegenden Arbeit möchten wir insbesondere einen Beweis der negativen Lösung von H10 führen. Grundsätzlich orientieren wir uns an der Argumentation in [Dav73], die meisten unserer Beweise finden sich in ähnlicher Form dort. Wir beschreiben kurz unsere Vorgehensweise:

Wir werden in Kapitel 2 zunächst einige Begriffe aus der Berechenbarkeitstheorie wiederholen und dann zeigen, dass diophantische Mengen rekursiv aufzählbar sind.
In Kapitel 3 entwickeln wir ein genaueres Verständnis davon, was diophantische Gleichungen, Mengen und Funktionen sind. Wir werden Beispiele betrachten und erste fundamentale und wichtige Methoden kennenlernen.
In Kapitel 4 widmen wir uns den diophantischen Ausdrücken. Wir untersuchen, wie wir diophantische Mengen beschreiben können und welche Operationen diophantische Ausdrücke darstellen. Nachdem wir erkennen, dass fast alles, was einen Nutzen für uns hat, durch diophantische Ausdrücke beschrieben werden kann, zeigen wir noch die Grenzen diophantischer Ausdrücke auf und zeigen damit, welche Mengen nicht diophantisch sind. Der Kern dieses Kapitels ist das Resultat, dass die Exponentialfunktion diophantisch ist. Für den Beweis dieser Aussage werden wir uns eingehend mit der Pell-Gleichung beschäftigen.
In Kapitel 5 lernen wir die rekursiven Funktionen kennen. Diese bilden ein Berechenbarkeitsmodell, das äquivalent zu den wohlbekannten Turingmaschinen ist (wir gehen kurz auf diese Äquivalenz ein). Wir zeigen, dass eine Funktion genau dann rekursiv ist, wenn sie diophantisch ist.
Die negative Lösung zu H10 liefern wir in Kapitel 6. Wir definieren die universelle diophantische Menge und konstruieren eine nicht-rekursive Funktion. Damit folgern wir, dass die Lösbarkeit diophantischer Gleichungen nicht entscheidbar ist. Dabei bilden die rekursiven Funktionen unser zentrales Hilfsmittel.
Schließlich betrachten wir in Kapitel 7 anhand verschiedener Beispiele die hypothetische Anwendung eines Algorithmus, der diophantische Mengen entscheiden kann. Dabei werden wir sehen, dass wir mit diophantischen Mengen bekannte, lange ungelöste und sogar zum Teil bis heute ungelöste Probleme beschreiben können. Ein Algorithmus zur Entscheidung diophantischer Mengen hätte also einige offene Frage bereits beantworten können.
Im Ausblick (8) betrachten wir kurz weitere Fragestellungen rund um Hilberts 10. Problem und erfahren dabei, dass einige davon sogar noch offen und ungelöst sind.

[6] Martin Davis (⋆1928) ist ein amerikanischer Mathematiker, der insbesondere für seine Arbeit zu Hilberts 10. Problem bekannt ist.
[7] Hilary Putnam (⋆1926, †2016) war ein amerikanischer Philosoph und Mathematiker, der zum Beweis der Unentscheidbarkeit diophantischer Mengen beitrug.
[8] Julia Robinson (⋆1919, †1985) war eine amerikanische Mathematikerin, die für ihre Arbeit an Entscheidungsproblemen sowie H10 bekannt ist.
[9] Yuri Matijasevič (⋆1947) ist ein russischer Mathematiker, der mit seiner negativen Antwort auf Hilberts 10. Problem im Alter von 22 Jahren bekannt wurde.

2 Entscheidbarkeit

In diesem Kapitel möchten wir einige Begriffe aus der Berechenbarkeitstheorie wiederholen. Dabei setzen wir grundlegende Kenntnisse über Turingmaschinen voraus, da diese im Folgenden weder definiert noch genauer beschrieben werden. Dafür verweisen wir auf die Literatur, beispielsweise [Sip06, Kapitel 3.1] und [HMU01, Kapitel 8.2]. Wir erinnern an einige Definitionen, die unser Verständnis des 10. Hilbertschen Problems verbessern sollen und zeigen, dass die Entscheidung diophantischer Mengen rekursiv aufzählbar ist (eine stärkere Aussage liefert Satz 6.7).

Definition 2.1. Eine Sprache L heißt *rekursiv aufzählbar* genau dann, wenn eine Turingmaschine existiert, die L erkennt.

Definition 2.2. Eine Turingmaschine M heißt *Entscheider*, falls M auf allen Eingaben stoppt.

Definition 2.3. Eine Sprache L heißt *entscheidbar* genau dann, wenn ein Entscheider existiert, der L erkennt.

Wir werden in Kapitel 5 ein alternatives und sogar äquivalentes Berechenbarkeitsmodell kennenlernen: die *rekursiven Funktionen*. Mithilfe der rekursiven Funktionen werden wir dann die Unentscheidbarkeit diophantischer Mengen beweisen. An dieser Stelle möchten wir zeigen, dass dieses Problem rekursiv aufzählbar ist (vgl. [Sip06, Abschnitt 3.3, S. 154 ff.]). Dazu formulieren wir Hilberts 10. Problem in Begriffen der Berechenbarkeitstheorie:

Definition 2.4. Betrachte für $n \geq 0$

$$D_n = \{p : p \text{ ist ein Polynom in den Variablen } x_1, \ldots, x_n \\ \text{mit Koeffizienten und Nullstellen in } \mathbb{Z}\}.$$

Die Entscheidung der Menge $D = \bigcup D_n$ ist Hilberts 10. Problem für beliebige Polynome mit Koeffizienten und Nullstellen in $\mathbb{Z}$.

Nach Abschnitt 6.2 ist dieses Problem nicht entscheidbar. Wir zeigen nun, dass D zumindest rekursiv aufzählbar ist:

Lemma 2.5. *D ist rekursiv aufzählbar.*

Beweis. Betrachte D_1. Die Entscheidung dieser Menge ist Hilberts 10. Problem für Polynome in einer Variablen x. Die Turingmaschine M_1 erkennt D_1:

$M_1 =$ „Bei Eingabe eines Polynoms über der Variablen x.

1. Werte das Polynom p nacheinander für die Werte $0, 1, -1, 2, -2, \ldots$ aus, bis das Polynom den Wert 0 ergibt, dann akzeptiere.“

Falls $p \in D_1$ eine ganzzahlige Nullstelle hat, so wird M_1 diese finden und akzeptieren. Falls nicht, so läuft M_1 immer weiter.

Für Polynome in mehreren Variablen können wir eine ähnliche Turingmaschine M angeben, die D erkennt:

$M =$ „Bei Eingabe eines Polynoms über den Variablen $x_1, \ldots, x_n$
1. Werte das Polynom p nacheinander für alle Kombinationen der Werte
$0, 1, -1, 2, -2, \ldots$ aus, bis das Polynom den Wert 0 ergibt, dann akzeptiere.“

M prüft alle möglichen Kombinationen ganzzahliger Werte für die Variablen des Polynoms. Diese Kombinationen können wir als Vektor auffassen. Zunächst prüft M, ob der Nullvektor eine Nullstelle des Polynoms ist. Danach verändern wir einen beliebigen Koeffizienten des Vektors zu einer Eins und prüfen jede mögliche Permutation. Als nächstes verändern wir einen weiteren Koeffizienten zu einer Eins und prüfen erneut jede mögliche Permutation und so weiter. Nachdem wir den Vektor, der nur aus Einsen besteht, geprüft haben, beginnen wir erneut mit dem Nullvektor und verändern die Koeffizienten schrittweise zu -1. Auf diese Weise betrachten wir nach und nach alle möglichen Lösungsvektoren in aufsteigender Reihenfolge bezüglich des Betrages der Koeffizienten (beispielhaft für ein Polynom in 2 Variablen: wir prüfen in folgender Reihenfolge: $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$, $(-1,0)$, $(0,-1)$, $(-1,-1)$, $(1,-1)$, $(-1,1)$, $(2,0)$, $\ldots$) Wir prüfen also dem Betrag nach immer größer werdende mögliche Nullstellen, bis wir erfolgreich sind und akzeptieren dann. Dabei wird jede mögliche Permutation geprüft, um keine mögliche Lösung zu überspringen.

Falls $p \in D$ eine ganzzahlige Nullstelle hat, so wird M diese finden und akzeptieren. Falls nicht, so läuft M immer weiter. Wir haben also eine Turingmaschine konstruiert, die die Menge D erkennt, also ist D rekursiv aufzählbar. □

Die Entscheidung der Lösbarkeit diophantischer Gleichungen ist also ein rekursiv aufzählbares, aber (nach Satz 6.4) kein entscheidbares Problem.

3 Diophantische Mengen und Funktionen

In diesem Kapitel beschäftigen wir uns mit einigen grundlegenden Begriffen und lernen erste hilfreiche Methoden kennen. Wir definieren diophantische Gleichungen, Mengen und Funktionen und betrachten Beispiele. Außerdem werden wir sehen, dass die Betrachtung von Hilberts 10. Problem über den natürlichen Zahlen äquivalent ist zur Betrachtung über den ganzen Zahlen. Aus diesem Grund werden wir die benötigten Begriffe direkt für Zahlen aus $\mathbb{N}$ definieren.

3.1 Grundbegriffe

Definition 3.1. Eine Gleichung heißt *diophantisch*, falls sie für ein Polynom P von der Form $P(x_1, \ldots, x_n) = 0$ ist. Dabei ist $P \in \mathbb{Z}[x_1, \ldots, x_n]$ und $\mathbb{Z}[x_1, \ldots, x_n]$ bezeichnet die Menge aller Polynome mit Koeffizienten aus dem Ring $\mathbb{Z}$ in den Variablen $x_1, \ldots, x_n$ versehen mit der üblichen Addition und Multiplikation.

Im 10. Hilbertschen Problem geht es um die Lösbarkeit diophantischer Gleichungen. Da liegt es nahe, sich genauer mit den Lösungen diophantischer Gleichungen zu beschäftigen. Anstatt diese zu einer gegebenen Gleichung zu suchen, betrachten wir eine Menge von Lösungen und suchen die zugehörige diophantische Gleichung. Solche Mengen bezeichnen wir als diophantische Mengen.

Definition 3.2. Eine Menge heißt *diophantisch*, wenn es ein Polynom

$$P(x_1, \ldots, x_n, y_1, \ldots, y_m) \text{ für } m \geq 0 \text{ und } x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathbb{N}$$

mit ganzzahligen Koeffizienten gibt, sodass S genau die n-Tupel enthält, für die $P = 0$ lösbar ist, d. h. wenn gilt:

$$\langle x_1, \ldots, x_n \rangle \in S \Leftrightarrow \exists y_1, \ldots, y_n : P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Beispiele 3.3. Wir betrachten einige Beispiele diophantischer Mengen. Dabei stehen alle Variablen für natürliche Zahlen.

i) Zahlen, die keine Zweierpotenzen sind:

$$x \in S \Longleftrightarrow \exists y, z(x - (2y + 3)z = 0).$$

ii) zusammengesetzte Zahlen:

$$x \in S \Longleftrightarrow \exists y, z(x - (y + 2)(z + 2) = 0).$$

iii) Ordnungsrelation $\mathbb{Z}^+$, d. h. $\{\langle x, y \rangle : x < y\}$ und $\{\langle x, y \rangle : x \leq y\}$:

$$x < y \Longleftrightarrow \exists z(x - y + z = 0),$$

$$x \leq y \Longleftrightarrow \exists z(x - y + z - 1 = 0).$$

iv) Teilbarkeitsrelation, d. h. $\{\langle x, y\rangle : x \mid y\}$:

$$x \mid y \iff \exists z(xz - y = 0).$$

v) Menge W der $\langle x, y, z\rangle$ mit $x \mid y$ und $x < z$ (wir kombinieren iii) und iv)):

$$\langle x, y, z\rangle \in W \iff \exists u, v((y - xu)^2 + (z - x - v)^2 = 0).$$

vi) Quadratzahlen:

$$x \in S \iff \exists y(x - y^2 = 0).$$

vii) Zahlen, die keine Quadratzahlen sind:

$$x \in S \iff \exists u, v, w((x - w^2 - u - 1)^2 + ((w + 1)^2 - x - v - 1)^2 = 0.$$

Später können wir mit stärkeren Methoden weitere Mengen diophantisch definieren.

Bemerkung 3.4. In Beispiel 3.3 v) haben wir ein System diophantischer Gleichungen auf eine einzelne diophantische Gleichung reduziert. Die genutzte Methode ist sehr einfach und funktioniert ganz allgemein für jegliche Gleichungssysteme der passenden Gestalt: Gegeben ein System von Gleichungen, formen wir jede dieser Gleichungen so um, dass sie gleich Null stehen. Wir können dieses System dann auf eine Gleichung reduzieren, indem wir die Summe der Quadrate der linken Seiten gleich Null schreiben, also:

$$P_1 = 0, \ldots, P_k = 0 \Longrightarrow P_1^2 + \cdots + P_n^2 = 0.$$

Diese Methode werden wir später noch dazu verwenden, um von einer Funktion zu zeigen, dass sie diophantisch ist.

Definition 3.5. Eine Funkion in n Variablen heißt *diophantisch*, wenn ihr Graph diophantisch ist, d. h. wenn die Menge $\{\langle x_1, \ldots, x_n, y\rangle : y = f(x_1, \ldots, x_n)\}$ diophantisch ist.

Wir werden nun auch erste Beispiele für diophantische Funktionen kennenlernen:

Satz 3.6. *(Cantor'sche Paarungsfunktion)*
Es gibt diophantische Funktionen $P(x, y)$, $L(z)$, $R(z)$ mit

1. *für alle x, y ist $L(P(x, y)) = x$, $R(P(x, y)) = y$,*
2. *für alle z ist $P(L(z), R(z)) = z$, $L(z) \leq z$, $R(z) \leq z$.*

Beweis.

Existenz

Betrachte den kleinen Gauß als Funktion

$$T(n) = 1 + 2 + \cdots + n = \frac{n(n + 1)}{2}.$$

Die Funktionswerte dieser Funktion sind die sogenannten Dreieckszahlen. $T(n)$ ist offensichtlich eine monoton wachsende Funktion, also gibt es für jedes $z \in \mathbb{N}^+$ ein eindeutiges $n \geq 0$ sodass gilt:

$$T(n) < z \leq T(n+1) = T(n) + n + 1.$$

Daher ist z eindeutig darstellbar als

$$z = T(n) + y = T(x + y - 2) + y + 1.$$

Wir schreiben

$$x = L(z), y = R(z)$$

und setzen

$$P(x, y) = T(x + y - 2) + y + 1.$$

Eigenschaften

Wir zeigen, dass L, R und P diophantisch sind:

$$\begin{aligned} z = P(x,y) &\iff \quad 2z = (x+y-2)(x+y-1) + 2y, \\ x = L(z) &\iff \exists y(2z = (x+y-2)(x+y-1) + 2y), \\ y = R(z) &\iff \exists y(2z = (x+y-2)(x+y-1) + 2y). \end{aligned}$$

Die Funktion $P(x, y)$ bildet die Menge der geordneten Paare natürlicher Zahlen injektiv auf die Menge der ganzen Zahlen ab.

Für jedes geordnete Paar z ist

$$P(x, y) = z \text{ mit } x = L(P(x, y)) \text{ und } y = R(P(x, y)).$$

Wir bemerken, dass $L(z) \leq z$ und $R(z) \leq z$ gilt.

□

Für das nächste Beispiel erinnern wir an zwei Sätze aus der Algebra:

Satz 3.7. *(Chinesischer Restsatz)* [Bos09, Satz 12, Korollar 13] *Für beliebige positive Zahlen $a_1, \ldots, a_n \in \mathbb{Z}^+$ und paarweise teilerfremde Zahlen $m_1, \ldots, m_n \in \mathbb{Z}^+$ gibt es eine Zahl $x \in \mathbb{Z}^+$, sodass gilt:*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n. \end{aligned}$$

Satz 3.8. *(Satz von Lagrange)* [Her75, Satz 7.4.1] *Jede positive ganze Zahl lässt sich als Summe der Quadrate vierer ganzer Zahlen schreiben.*

Definition 3.9. Wir definieren die *Nachfolgerfunktion* $S(i,u)$ durch $S(i,u) = w$, wobei w die eindeutige natürliche Zahl ist mit

$$\begin{aligned} w &\equiv L(u) \mod iR(u)+1 \\ &\text{und } w \leq iR(u)+1. \end{aligned}$$

In diesem Fall ist w der kleinste positive Rest der Division von $L(u)$ geteilt durch $iR(u)+1$.

Satz 3.10. *(Satz über die Nachfolgerfunktion) Es gibt eine diophantische Funktion $S(i,u)$ wie in Definition 3.9, sodass gilt:*

1. $S(i,u) \leq u$,
2. *für jede Folge $a_1, \ldots, a_n$ mit $a_i \in \mathbb{N}^+$ für alle $i \in \mathbb{N}$ gibt es eine Zahl u mit $S(i,u) = a_i$ für $1 \leq i \leq n$.*

Beweis. Zuerst zeigen wir, dass $S(i,u)$ aus Definition 3.9 diophantisch ist. Dazu soll die Gleichung $w = S(i,u)$ genau dann gelten, wenn das folgende System von Gleichungen eine Lösung hat:

$$\begin{aligned} 2u &= (x+y-2)(x+y-1)+2y \qquad \text{(i)} \\ x &= w + z(iy+1) \\ iy+1 &= w+v-1 \end{aligned}$$

Dies folgt (analog zur Argumentation im Beweis von 3.6), da Gleichung (i) äquivalent ist zu

$$x = L(u) \text{ und } y = R(u).$$

Nach dem Satz von Lagrange (3.8) ist dann $S(i,u)$ diophantisch. Es ist $S(i,u) \leq L(u) \leq u$, womit wir Eigenschaft 1 gezeigt haben.
Seien also $a_1, \ldots, a_n$ gegeben. Wähle ein $y > \max\{a_1, \ldots, a_n\}$, das durch jede der Zahlen $1, 2, \ldots, n$ teilbar ist. Dann sind die Zahlen $1+y, 1+2y, \ldots, 1+ny$ paarweise teilerfremd, denn:
Falls $d \mid 1+iy$ und $d \mid 1+jy$ mit $i < j$, so ist $d \mid j(1+iy) - i(1+jy)$, also ist $d \mid j-1$ und somit $d \leq n$, aber da $d = 1$ wegen $d \mid y$ ist, ist das nicht möglich.
Der Chinesische Restsatz (3.7) liefert uns in diesem Fall ein x mit

$$\begin{aligned} x &\equiv a_1 \mod y+1 \\ x &\equiv a_2 \mod 2y+1 \\ &\vdots \\ x &\equiv a_n \mod ny+1. \end{aligned}$$

Sei $u = P(x,y)$, sodass $x = L(u)$ und $y = R(u)$. Dann ist für $i = 1, 2, \ldots, n$

$$a_i \equiv L(u) \mod iR(u)+1$$

und $a_i < y = R(u) < iR(u)+1$, und nach Definition ist $a_i = S(i,u)$, was uns Eigenschaft 2 liefert und den Beweis vervollständigt. □

Wir lernen nun eine weitere Charakterisierung von diophantischen Mengen kennen. Das folgende Theorem stammt von Hilary Putnam.

Satz 3.11. *Sei S eine Menge positiver ganzer Zahlen. Dann ist S genau dann diophantisch, wenn es ein Polynom $P \in \mathbb{Z}[y_0, \ldots, y_m]$ gibt mit*

$$S = \{x \in \mathbb{N} : \exists x_0, \ldots, x_m \in \mathbb{N}\ P(x_0, \ldots, x_m) = x\},$$

d. h. S ist die Menge der positiven Zahlen im Bild von P eingeschränkt auf $\mathbb{N}^n$.

Beweis.

„⇒“: Sei S diophantisch und $x > 0$ für alle $x \in S$. Dann existiert $Q \in \mathbb{Z}[y_0, \ldots, y_m]$ mit

$$x \in S \iff \exists x_1, \ldots, x_m\ Q(x, x_1, \ldots, x_m) = 0.$$

Betrachte

$$P(y_0, \ldots, y_m) := [1 - Q(y_0, y_1, \ldots, y_m)^2]y_0.$$

Dann gilt für $x \in S$ und $x_1, \ldots, x_m \in \mathbb{N}$ mit $Q(x, x_1, \ldots, x_m) = 0$ auch

$$P(x_0, \ldots, x_m) = x_0,\ \text{d. h. } x \in \{x \in \mathbb{N} : \exists x_0, \ldots, x_m \in \mathbb{N}\ P(x_0, \ldots, x_m) = x\}.$$

Sei $y \in \{x \in \mathbb{N} : \exists x_0, \ldots, x_m \in \mathbb{N}\ P(x_0, \ldots, x_m) = x\}$, d. h. es gibt $x_0, \ldots, x_m \in \mathbb{N}$ mit $P(x_0, \ldots, x_m) = y$. Dann gilt

$$y = [1 - Q(x_0, \ldots, x_m)^2]x_0.$$

Da $y > 0$ gilt $x_0 > 0$ und wegen $1 - Q(x_0, \ldots, x_m)^2 > 0$ ist $1 - Q(x_0, \ldots, x_m)^2 = 1$. Also gilt

$$x_0 = y \text{ und } Q(x_0, \ldots, x_m) = 0.$$

„⇐“: Sei $S = \{x \in \mathbb{N} : \exists x_1, \ldots, x_m \in \mathbb{N}\ P(x_1, \ldots, x_m) = x\}$ und es gelte $x > 0$ für alle $x \in S$.

Betrachte $\tilde{Q}(y_0, \ldots, y_m) := P(y_1, \ldots, y_m) - y_0$. Dann gilt für $x_0, \ldots, x_m \in \mathbb{N}$

$$\tilde{Q}(x_0, \ldots, x_m) = 0 \iff P(x_1, \ldots, x_m) = x_0.$$

□

3.2 Diophantische Gleichungen über den natürlichen Zahlen

Wir möchten kurz darauf eingehen, warum es ausreicht, H10 über $\mathbb{N}$ zu betrachten, obwohl Hilbert sein Problem über $\mathbb{Z}$ formuliert hat. Mit H10 über $\mathbb{N}$ bezeichnen wir die Entscheidung der Lösbarkeit von Gleichungen mit Koeffizienten und Lösungen in $\mathbb{N}$. Der Beweis folgt der Argumentation in [Mat96, S. 3 f.].

Satz 3.12. *(Äquivalenz der Probleme über $\mathbb{N}$ und $\mathbb{Z}$) Bei der Lösung von Hilberts 10. Problem spielt es keine Rolle, ob wir die Lösungen der diophantischen Gleichungen (mit ganzzahligen Koeffizienten) über $\mathbb{N}$ oder $\mathbb{Z}$ betrachten, beide Probleme sind äquivalent:*

Algorithmus für Lösungen über $\mathbb{N}$ $\Leftrightarrow$ Algorithmus für Lösungen über $\mathbb{Z}$.

Beweis.

„⇒“: Angenommen, wir haben einen Algorithmus, der H10 über $\mathbb{N}$ entscheidet, und suchen eine ganzzahlige Lösung für

$$P(x_1, \ldots, x_n) = 0. \tag{1}$$

Dann betrachten wir die Gleichung

$$P(p_1 - q_1, \ldots, p_n - q_n) = 0. \tag{2}$$

Offenbar ist jede Lösung von (2) in den natürlichen Zahlen $p_1, \ldots, p_n, q_1, \ldots, q_n$ auch eine Lösung von (1) in den ganzen Zahlen $x_1, \ldots, x_n$ durch

$$\begin{aligned} x_1 &= p_1 - q_1 \\ &\vdots \\ x_n &= p_n - q_n. \end{aligned} \tag{3}$$

Umgekehrt finden wir für jede Lösung $x_1, \ldots, x_n$ von (1) natürliche Zahlen $p_1, \ldots, p_n$, $q_1, \ldots, q_n$, die (3) erfüllen und dadurch eine Lösung $p_1 - q_1, \ldots, p_n - q_n$ von (2) bilden.

„⇐“: Angenommen, wir haben einen Algorithmus, der H10 über $\mathbb{Z}$ entscheidet, und suchen natürliche Lösungen für

$$P(y_1, \ldots, y_n) = 0. \tag{4}$$

Dann betrachten wir die Gleichung

$$P(a_1^2 + b_1^2 + c_1^2 + d_1^2, \ldots, a_n^2 + b_n^2 + c_n^2 + d_n^2) = 0. \tag{5}$$

Offenbar ist jede Lösung in $\mathbb{Z}$ von (5) schon eine Lösung in $\mathbb{N}$ von (4). Umgekehrt können wir jede Lösung von (4) in natürlichen Zahlen $y_1, \ldots, y_n$ nach dem Satz von Lagrange (3.8) als eine Lösung von (5) in ganzen Zahlen $a_1, b_1, c_1, d_1, \ldots, a_n, b_n, c_n, d_n$ schreiben.

□

Um die Betrachtung zu vereinfachen, beschränken wir von nun an unsere Untersuchung auf Lösungen diophantischer Gleichungen über $\mathbb{N}$.

4 Diophantische Ausdrücke

In diesem Kapitel betrachten wir Ausdrücke, mit denen diophantische Mengen beschrieben werden können, sogenannte diophantische Ausdrücke.
Zunächst werden wir sehen, dass die Exponentialfunktion diophantisch ist, also durch einen diophantischen Ausdruck beschrieben werden kann. Darauf aufbauend werden wir weitere Funktionen und Mengen betrachten, die sich durch diophantische Ausdrücke beschreiben lassen.

Definition 4.1. Wir betrachten das folgende System diophantischer Gleichungen

$$x^2 - (a^2-1)y^2 = 1 \tag{I}$$
$$u^2 - (a^2-1)v^2 = 1 \tag{II}$$
$$s^2 - (b^2-1)t^2 = 1 \tag{III}$$
$$v = ry^2 \tag{IV}$$
$$b = 1 + 4py = a + qu \tag{V}$$
$$s = x + cu \tag{VI}$$
$$t = k + 4(d-1)y \tag{VII}$$
$$y = k + e - 1 \tag{VIII}$$

für ganze Zahlen $a, b, c, d, e, k, p, q, r, s, t, u, v, x, y$ mit $a > 1$. Wir bezeichnen dieses System kurz mit (I-VIII).

4.1 Die Pell-Gleichung

Bevor wir uns der Exponentiation widmen können, benötigen wir einige Hilfssätze. Dazu betrachten wir die *Pell-Gleichung* und beschäftigen uns mit ihren Lösungen und Eigenschaften ihrer Lösungen.

Definition 4.2. Seien $x, y \geq 0$ und $d = a^2 - 1$ sowie $a > 1$ für $a \in \mathbb{Z}^+$. Dann heißt folgende Gleichung die *Pell-Gleichung*

$$x^2 - dy^2 = 1. \tag{P}$$

Wir bemerken, dass die Gleichungen (I), (II) und (III) jeweils Pell-Gleichungen sind.

Bemerkung 4.3. Betrachte

$$x_0 := 1, \quad y_0 := 0,$$
$$x_1 := a, \quad y_1 := 1.$$

Offensichtlich sind durch x_0, y_0 und x_1, y_1 Lösungen von (P) gegeben.

Da wir jetzt wissen, was die Pell-Gleichung ist, können wir uns etwas eingehender mit ihr beschäftigen. Wir möchten einige Eigenschaften ihrer Lösungen beweisen und werden Parallelen zu bekannten Gleichungen und Funktionen entdecken.

Für eine natürliche Zahl d möchten wir mit $\sqrt{d}$ die positive Wurzel notieren, also die positive reelle Zahl, die zur zweiten Potenz d ergibt.

Lemma 4.4. *Falls x, y ganzzahlige Lösungen der Pell-Gleichung sind, dann gilt*

$$x + y\sqrt{d} \leq 1 \text{ oder } x + y\sqrt{d} \geq a + \sqrt{d}.$$

Beweis. Wir führen den Beweis per Widerspruch, also nehmen wir an, dass es eine ganzzahlige Lösung (x, y) von (P) gibt, für die gilt:

$$1 < x + y\sqrt{d} < a + \sqrt{d}.$$

Aus der Pell-Gleichung erhalten wir

$$\begin{aligned} x^2 - dy^2 &= 1 \\ \iff (x + y\sqrt{d})(x - y\sqrt{d}) &= 1 \end{aligned}$$

und

$$\begin{aligned} a^2 - 1 &= d \\ \iff a^2 - d &= 1 \\ \iff (a + \sqrt{d})(a - \sqrt{d}) &= 1. \end{aligned}$$

Es gilt also

$$(x + y\sqrt{d})(x - y\sqrt{d}) = (a + \sqrt{d})(a - \sqrt{d}) = 1.$$

Unsere Annahme liefert:

$$1 > x - y\sqrt{d} > a - \sqrt{d}.$$

Der Kehrwert ist dann:

$$-1 < -x + y\sqrt{d} < -a + \sqrt{d}.$$

Zusammen erhalten wir

$$0 < 2y\sqrt{d} < 2\sqrt{d}, \text{ also } 0 < y < 1,$$

im Widerspruch zur Annahme. Also gilt

$$x + y\sqrt{d} \leq 1 \text{ oder } x + y\sqrt{d} \geq a + \sqrt{d}.$$

□

Lemma 4.5. *Seien x, y und x', y' ganzzahlige Lösungen von (P). Sei*

$$x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d}),$$

dann sind auch x'', y'' Lösungen der Pell-Gleichung.

Beweis. Wir betrachten die Konjugierte $x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d})$. Die Multiplikation der beiden Gleichungen ergibt $(x'')^2 - d(y'')^2 = (x^2 - dy^2)((x')^2 - d(y')^2) = 1$. Damit erfüllen x'', y'' die Pell-Gleichung. □

Definition 4.6. Wir definieren die Zahlen $x_n(a)$, $y_n(a)$ für $n \geq 0$, $a > 1$ durch $x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$.

Korollar 4.7. *Die Zahlen $x_n(a)$, $y_n(a)$ sind Lösungen von (P).*

Beweis. Das folgt per Induktion aus Lemma 4.5. □

Lemma 4.8. *Seien x, y nichtnegative Lösungen der Pell-Gleichung. Dann gibt es ein n, sodass gilt $x = x_n(a)$, $y = y_n(a)$.*

Beweis. Wir schreiben kurz $x_n := x_n(a)$ und $y_n := y_n(a)$. Falls $x + y\sqrt{d} < 1$ gilt, so sind die Lösungen x und y negativ. Wir möchten nur nichtnegative Lösungen betrachten, also nehmen wir an, dass $x + y\sqrt{d} \geq 1$ gilt. Da $(a + \sqrt{d})^n$ für wachsendes n unendlich groß wird, gibt es ein $n \geq 0$, sodass gilt

$$(a + \sqrt{d})^n \leq x + y\sqrt{d} < (a + \sqrt{d})^{n+1}.$$

Die Behauptung ist bewiesen, falls gilt:

$$(a + \sqrt{d})^n = x + y\sqrt{d}.$$

Wir nehmen also an, dass gilt:

$$(a + \sqrt{d})^n < x + y\sqrt{d}.$$

Dann gilt

$$x + y\sqrt{d} < (x_n + y_n\sqrt{d})(a + \sqrt{d}) = (a + \sqrt{d})^{n+1}.$$

Wegen

$$(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = 1$$

ist

$$x_n - y_n\sqrt{d} > 0.$$

Also gilt

$$1 < (x + y\sqrt{d})(x_n - y_n\sqrt{d}) < a + \sqrt{d},$$

im Widerspruch zu Lemma 4.4 und Lemma 4.5.

□

Wir haben an dieser Stelle eine Analogie zur Euler-Formel kennengelernt. Diese lautet bekanntlich

$$(\cos u) + (\sin u)\sqrt{-1} = e^{iu}.$$

Die Relation $x_n + y_n\sqrt{d} = (a+\sqrt{d})^n$ ist dann ein Analogon, wobei wir x_n statt cos und y_n statt sin haben. Statt -1 haben wir an geeigneten Stellen d und erhalten auf diese Weise weitere Analogien zu bekannten Formeln.
So bildet die Pell-Gleichung

$$x_n^2 - dy_n^2 = 1$$

eine Analogie zum Trigonometrischen Pythagoras

$$\sin^2\alpha + \cos^2\alpha = 1.$$

Wir werden später sehen, dass die Lösungen von (P) vergleichbar mit sin und cos auch periodische Eigenschaften besitzen. Außerdem erhalten wir auch für die Lösungen der Pell-Gleichung gewisse Additionstheoreme, wie das folgende Lemma zeigt.

Lemma 4.9. *Es gilt $x_{m\pm n} = x_m x_n \pm d y_n y_m$ und $y_{m\pm n} = x_n y_m \pm x_m y_n$. Insbesondere gilt $y_{m\pm 1} = a y_m \pm x_m$ und $x_{m\pm 1} = a x_m \pm d y_m$.*

Beweis. Es gilt

$$\begin{aligned} x_{m+n} + y_{m+n}\sqrt{d} &= (a+\sqrt{d})^{m+n} \\ &= (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= (x_m x_n + d y_m y_n) + (x_n y_m + x_m y_n)\sqrt{d}. \end{aligned}$$

Also ist

$$x_{m+n} = x_m x_n + d y_m y_n$$

und

$$y_{m+n} = x_n y_m + x_m y_n.$$

Weiter gilt

$$\begin{aligned} x_{m-n} + y_{m-n}\sqrt{d} &= (a+\sqrt{d})^{m-n} \\ &= \frac{x_m + y_m\sqrt{d}}{x_n + y_n\sqrt{d}} \end{aligned}$$

und

$$x_m + y_m\sqrt{d} = (x_{m-n} + y_{m-n}\sqrt{d})(x_n + y_n\sqrt{d}).$$

Wir erhalten

$$\begin{aligned} x_{m-n} + y_{m-n}\sqrt{d} &= (x_m + y_m\sqrt{d})(x_n - y_n\sqrt{d}) \\ &= (x_m x_n - d y_m y_n)(x_n y_m - x_m y_n)\sqrt{d}. \end{aligned}$$

Also gilt

$$x_{m-n} = x_m x_n - d y_n y_m$$

und

$$y_{m-n} = x_n y_m - x_m y_n.$$

□

Lemma 4.10. *Es gilt* $x_{n+1} = 2ax_n - x_{n-1}$ *und* $y_{n+1} = 2ay_n - y_{n-1}$.

Beweis. Nach Lemma 4.9 gilt

$$\begin{aligned} x_{n+1} &= ax_n + dy_n, \\ x_{n-1} &= ax_n - dy_n, \\ y_{n+1} &= ay_n + x_n, \\ y_{n-1} &= ay_n - x_n. \end{aligned}$$

Also ist $x_{n+1} + x_{n-1} = 2ax_n$ und damit $x_{n+1} = 2ax_n - x_{n-1}$; sowie $y_{n+1} + y_{n-1} = 2ay_n$ und damit $y_{n+1} = 2ay_n - y_{n-1}$. □

Diese Rekursionsgleichungen zweiter Ordnung liefern uns mit den Startwerten aus Bemerkung 4.3 alle Werte der x_n, y_n. Diverse Eigenschaften dieser Folgen lassen sich nun induktiv mithilfe dieser Werte für $n = 0$ und $n = 1$ beweisen.

Lemma 4.11. *Es gilt* $y_n \equiv n \mod a - 1$.

Beweis. Für $n = 0$ und $n = 1$ gilt die Kongruenz. Induktiv folgt (mit $a \equiv 1 \mod a - 1$): $y_{n+1} = 2ay_n - y_{n-1} \equiv 2n - (n-1) \mod a - 1$. □

Lemma 4.12. *Es gilt* $x_n(a) - y_n(a)(a - y) \equiv y^n \mod 2ay - y^2 - 1$.

Beweis. Für $n = 0$ ist $x_0 - y_0(a - y) = 1$ und für $n = 1$ ist $x_1 - y_1(a - y) = y$.
Mit Lemma 4.10 folgt induktiv:

$$\begin{aligned} x_{n+1} - y_{n+1}(a - y) &= 2a(x_n - y_n(a - y)) - (x_{n-1} - yn - 1(a - y)) \\ &\equiv 2ay^n - y^{n-1} \\ &= y^{n-1}(2ay - 1) \\ &\equiv y^{n-1}y^2 \\ &= y^{n+1}. \end{aligned}$$

□

Lemma 4.13. *Es gilt* $x_{n+1}(a) > x_n(a) \geq a^n$ *und* $x_n(a) \leq (2a)^n$ *für alle* n.

Beweis. Nach Lemma 4.9 und Lemma 4.10 ist $ax_n(a) \leq x_{n+1}(a) \leq (2a)x_n(a)$.
Die Behauptung folgt dann per Induktion. □

4.2 Exponentiation

Nachfolgend werden wir beweisen, dass die Exponentiation durch einen diophantischen Ausdruck beschrieben werden kann.

Satz 4.14. *Angenommen, die ganzen Zahlen a, x, k sind gegeben und es ist $a > 1$ sowie $p, q, r, u, y \geq 1$. Dann sind äquivalent:*

1. *Das System (I-VIII) hat eine Lösung in $\mathbb{N}$ in den verbleibenden Argumenten,*
2. *$x = x_k(a)$.*

Beweis. „(1) $\implies$ (2)“:
Angenommen, wir haben eine Lösung zu (I-VIII).Wir zeigen, dass dann $x = x_k(a)$ gilt. Nach (V) ist $b > a > 1$. Lemma 4.8 liefert uns $i, j, n > 0$ mit $x = x_i(a)$, $y = y_i(a)$, $u = x_n(a)$, $v = y_n(a)$, $s = x_j(b)$ und $t = y_j(b)$. Nach (IV) ist $y \leq v$, also ist auch $i \leq u$. Wegen der Gleichungen (V) und (VI) gilt

$$\begin{aligned} b &\equiv a \mod x_n(a) \\ x_j(b) &\equiv x_i(a) \mod x_n(a). \end{aligned}$$

***Behauptung A*:** Wir betrachten die Lösungen $x_n(a)$ und $y_n(a)$ von (P). Falls $a \equiv b \mod c$, dann gilt für alle n mit $x_n(a) \equiv x_n(b)$ die Kongruenz

$$y_n(a) \equiv y_n(b) \mod c.$$

Beweis: Für $n = 0$ und $n = 1$ haben wir Gleichheit. Induktiv folgt:

$$y_{n+1} \overset{4.10}{=} 2ay_n(a) - y_{n-1}(a) \equiv 2by_n(b) - y_{n-1}(b) \mod c = y_{n+1}(b).$$

■

Nach Behauptung A erhalten wir $x_j(b) \equiv x_j(a) \mod x_n(a)$ und daher ist

$$x_i(a) \equiv x_j(a) \mod x_n(a).$$

Als nächstes zeigen wir, dass $j \equiv \pm i \mod 4n$ gilt.

***Behauptung B*:** Falls $0 < i \leq n$ und $x_j \equiv x_i \mod x_n$, dann gilt $j \equiv \pm i \mod 4n$.

Beweis: Wir nähern uns dieser Behauptung schrittweise.

1. Schritt
Nach Lemma 4.9 und den oben gezeigten Konvergenzen gilt:

$$\begin{aligned} x_{2n\pm j} &= x_n x_{n\pm j} + dy_n y_{n\pm j} \\ &\equiv dy_n(y_n x_j \pm x_n y_j) \mod x_n \\ &\equiv dy_n^2 x_j \mod x_n \\ &= (x_n^2 - 1)x_j \\ &\equiv -x_j \mod x_n. \end{aligned}$$

Also gilt $x_{2n\pm j} \equiv -x_j \mod x_n$.
Dann ist auch $x_{4n\pm j} \equiv -x_{2n\pm j} \equiv x_j \mod x_n$.

2. Schritt
Angenommen, es gelte $a \neq 2$ oder $n \neq 1$ oder $i \neq 0$ oder $j \neq 2$.
Falls $x_i \equiv x_j \mod x_n$ mit $i \leq j \leq 2n$, $n > 0$ gilt, dann gilt $i = j$.

Wir unterscheiden, ob x_n gerade oder ungerade ist.

> **1. Fall** x_n ist ungerade:
> Sei $q = (x_n - 1)/2$, dann sind die Zahlen $-q, -q+1, \ldots, -1, 0, 1, \ldots, q-1, q$ eine vollständige Menge paarweise inkongruenter Reste modulo x_n. Nach Lemma 4.13 ist $1 = x_0 < x_1 < \cdots < x_{n-1}$.
>
> Dann ist nach Lemma 4.9 $x_{n-1} \leq x_n/a \leq \frac{1}{2}x_n$, also $x_{n-1} \leq q$. Nach Schritt 1 sind die Zahlen $x_{n+1}, x_{n+2}, \ldots, x_{2n-1}, x_{2n}$ kongruent modulo x_n zu $-x_{n-1}$, $-x_{n-2}$, $\ldots$, $-x_1, -x_0 = -1$. Also sind die Zahlen $x_0, \ldots, x_{2n}$ paarweise inkongruent modulo x_n, woraus $i = j$ folgt.
>
> **2. Fall** x_n ist gerade:
> Sei $q = x_n/2$, dann sind die Zahlen $-q+1, -q+2, \ldots, -1, 0, 1, \ldots q-1, q$ eine vollständige Menge paarweise inkongruenter Reste modulo x_n (denn es gilt $-q \equiv q \mod x_n$). Wie oben gilt $x_{n-1} \leq q$, also folgt $i = j$ wie oben.

Angenommen, es gelte $a = 2$, $n = 1$, $i = 0$ und $j = 2$. Dann ist $i = n - 1$ und $j = n + 1$. Nach Lemma 4.9 ist $x_n = ax_{n-1} + dy_{n-1}$, also ist $x_n = 2x_{n-1}$. Es folgt, dass $x_{n-1} = q - x_n/2$ und damit $x_{n+1} \equiv -q \mod x_n$ gilt. In diesem Fall gilt $i = j$ nicht, daher haben wir das sofort ausgeschlossen. Diesen Fall wollen wir als den *Ausnahmefall* bezeichnen.

3. Schritt
Wir zeigen: Falls $x_j \equiv x_i \mod x_n$ für $n > 0$, $0 < i \leq n$ und $0 \leq j < 4n$,
dann gilt $j = i$ oder $j = 4n - 1$.

> **1. Fall** $j \leq 2n$:
> Nach Schritt 2 ist $j = i$, außer im Ausnahmefall. Wegen $i > 0$ tritt dieser nur für $j = 0$ auf, doch dann ist $i = 2 > 1 = n$.
>
> **2. Fall** $j > 2n$:
> Sei $\bar{j} = 4n - j$, also $0 < \bar{j} < 2n$. Nach Schritt 1 ist $x_{\bar{j}} \equiv x_j \equiv x_i \mod x_n$. Wieder ist $\bar{j} = i$, außer im Ausnahmefall von Schritt 2. Wegen $i, \bar{j} > 0$ tritt dieser jedoch nicht auf.

4. Schritt
Nun zeigen wir: falls $0 < i \leq n$ und $x_j \equiv x_i \mod x_n$, dann gilt $j \equiv \pm i \mod 4n$.

> Setze $j = 4nq + \bar{j}$ mit $0 \leq \bar{j} < 4n$. Nach Schritt 1 ist $x_i \equiv x_j \equiv x_{\bar{j}} \mod x_n$. Nach Schritt 3 ist $i = \bar{j}$ oder $i = 4n - \bar{j}$, also ist $j \equiv \bar{j} \equiv \pm i \mod 4n$.

■

Also gilt nach Behauptung B

$$j \equiv \pm i \mod 4n. \tag{1}$$

Gleichung IV liefert $y_i^2(a) \mid y_n(a)$. Wir zeigen, dass dann schon $y_i(a) \mid n$ gilt.

***Behauptung C*:** Wir betrachten die Zahlen $y_n(a)$ und $y_t(a)$ für $n, t \geq 0$ und $a > 1$ wie in Definition 4.6. Wir schreiben kurz $x_n := x_n(a)$ und $y_n := y_n(a)$. Falls $y_n^2 \mid y_t$ gilt, dann gilt $y_n \mid t$.

Beweis: Wir nähern uns dieser Behauptung schrittweise.

1. Schritt
Wir zeigen, dass $\mathrm{ggT}(x_n, y_n) = 1$ gilt:

Falls $d \mid x_n$ und $d \mid y_n$ gilt, dann gilt auch $d \mid x_n^2 - dy_n^2$, also folgt $d \mid 1$.

2. Schritt
Wir zeigen, dass $y_n \mid y_{nk}$ gilt: Für $k = 1$ ist das offensichtlich.
Induktiv folgt mit Lemma 4.9

$$y_{n(m+1)} = x_n y_{nm} + x_{nm} y_n.$$

Nach Induktionsvoraussetzung ist $y_n \mid y_{nm}$, also gilt $y_n \mid y_{n(m+1)}$.

3. Schritt
Wir zeigen, dass $y_n \mid y_t \iff n \mid t$ gilt:

„$\Rightarrow$“: nach Schritt 2.

„$\Leftarrow$“: Angenommen, $y_n \mid y_t$, aber $n \nmid t$. Dann können wir $t = nq + r$, $0 < r < n$ schreiben. Dann ist $y_t = x_r y_{nq} + x_{nq} y_r$. Wegen Schritt 2 ist $y_n \mid y_{nq}$ und daher ist $y_n \mid x_{nq} y_r$. Jedoch gilt $\mathrm{ggT}(y_n, x_{nq}) = 1$, denn falls $d \mid y_n$ und $d \mid x_{nq}$ gilt nach Schritt 2 auch $d \mid y_{nq}$ und daher ist $d = 1$ nach Schritt 1. Also ist $y_n \mid y_r$, aber wegen $r < n$ ist $y_r < y_n$ nach Lemma 4.9, ein Widerspruch.

4. Schritt
Wir zeigen, dass $y_{nk} \equiv k x_n^{k-1} y_n \mod y_n^3$ gilt:

$$\begin{aligned} x_{nk} + y_{nk}\sqrt{d} &= (a + \sqrt{d})^{nk} \\ &= (x_n + y_n\sqrt{d})^k \\ &= \sum_{j=0}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{j/2}, \end{aligned}$$

also ist

$$y_{nk} = \sum_{\substack{j=1 \\ \text{j ungerade}}} \binom{k}{j} x_n^{k-j} y_k^j d^{(j-1)/2}.$$

Alle Terme dieser Entwicklung sind für $j > 1$ kongruent 0 modulo y_n^3.

5. Schritt
Nun zeigen wir: falls $y_n^2 \mid y_t$ gilt, dann gilt $y_n \mid t$.

Nach Schritt 3 ist $n \mid t$. Setze $t = nk$. Nach Schritt 4 ist $y_n^2 \mid kx_n^{k-1}y_n$, also ist $y_n \mid kx_n^{k-1}$. Aber nach Schritt 1 ist $\mathrm{ggT}(x_n, y_n) = 1$, also ist $y_n \mid k$ und daher ist $y_n \mid t$.

■

Also gilt $y_i(a) \mid n$ und (1) liefert

$$j \equiv \pm i \mod 4y_i(a). \tag{2}$$

Nach Gleichung (V) ist $b \equiv 1 \mod 4y_i(a)$ und dann ist

$$y_j(b) \equiv j \mod 4y_i(a), \tag{3}$$

was wir als nächstes zeigen werden.

***Behauptung D*:** Es gilt $y_n \equiv n \mod a - 1$.

Beweis: Für $n = 0$ und $n = 1$ herrscht Gleichheit.
Induktiv folgt mit $a \equiv 1 \mod a - 1$:

$$y_{n+1} \overset{4.10}{=} 2ay_n - y_{n-1} \equiv 2n - (n-1) \mod a - 1.$$

■

Nach (VII) ist

$$y_j(b) \equiv k \mod 4y_i(a) \tag{4}$$

und dann ergeben (2), (3) und (4) zusammen

$$k \equiv \pm i \mod 4y_i(a). \tag{5}$$

Gleichung (VIII) liefert uns $k \leq y_i(a)$ und wir zeigen, dass dann $i \leq y_i(a)$ ist.

***Behauptung E*:** Es gilt $y_{n+1} > y_n \geq n$ für alle n.

Beweis: Nach Lemma 4.9 ist $y_{n+1} > y_n$. Wegen $y_0 = 0 \geq 0$ folgt die Behauptung induktiv. ■

Da die Zahlen $-2y+1, -2y+2, \ldots, -1, 0, 1, \ldots, 2y-1, 2y$ eine vollständige Menge inkongruenter Reste modulo $4y = 4y_i(a)$ bilden, folgt mit diesen Ungleichungen aus (5) schon $k = i$. Also ist $x = x_i(a) = x_k(a)$.

„(2) $\implies$ (1)“:
Sei $x = x_k(a)$. Wir zeigen, dass dann das System (I-VIII) gilt. Wähle $y = y_k(a)$ so, dass (I) gilt. Setze $m = 2ky_k(a)$ und $u = x_m(a)$, $v = y_m(a)$, dann gilt (II). Wir zeigen, dass $y^2 \mid v$ gilt.

> ***Behauptung F*:** Es gilt $y_n^2 \mid y_{ny_n}$.
>
> Beweis: Setze $k = y_n$ in Schritt 4 im Beweis von Behauptung C. ■

Nach Schritt 3 im Beweis von Behauptung C und Behauptung F folgt jetzt $y^2 \mid v$. Daher können wir ein r wählen, sodass (IV) gilt.

> ***Behauptung G*:** Für gerade n ist y_n gerade und für ungerade n ist y_n ungerade.
>
> Beweis: Es ist
>
> $$y_{n+1} = 2ay_n - y_{n-1} \equiv y_{n-1} \mod 2.$$
>
> Für gerade n ist
>
> $$y_n \equiv y_0 = 0 \mod 2.$$
>
> Für ungerade n ist
>
> $$y_n \equiv y_1 = 1 \mod 2.$$
>
> ■

Nach Behauptung G ist v gerade, also ist u ungerade. Nach Schritt 1 im Beweis von C ist $\mathrm{ggT}(u, v) = 1$, also $\mathrm{ggT}(u, v4y) = 1$, denn falls p Primteiler von u und $4y$ ist, dann ist $p \mid y$, weil u gerade ist. Damit gilt $p \mid v$ wegen $y \mid v$.
Nach dem Chinesischen Restsatz (3.7) finden wir ein b_0 mit

$$\begin{aligned} b_0 &\equiv 1 \mod 4y \\ b_0 &\equiv a \mod u. \end{aligned}$$

Da auch $b_0 + 4juy$ diese Kongruenzen erfüllt, können wir b, p und q finden, sodass (V) gilt. Durch $s := x_k(b)$, $t := y_k(b)$ gilt auch (III). Wegen $b > a$ ist $s = x_k(b) > x_k(a) = x$. Nach Behauptung A liefert (V) $s \equiv x \mod u$, also können wir ein c wählen, sodass (VI) gilt. Nach Behauptung E ist $t \geq k$ und nach Lemma 4.11 ist $t \equiv k \mod b - 1$ und mit (V) ist $t \equiv k \mod 4y$, also können wir ein d wählen, sodass (VII) gilt. Nach Behauptung E ist $y \geq k$, also wird (VIII) durch $e := y - k + 1$ erfüllt. Damit ist das System (I-VIII) erfüllt. □

Korollar 4.15. *Die Funktion $g(z, k) = x_k(z + 1)$ ist diophantisch.*

Beweis. Wir erweitern das System (I-VIII) um die Gleichung

$$a = z + 1. \tag{A}$$

Nach Satz 4.14 ist das System (A, I-VIII) genau dann lösbar, wenn $x = x_k(a) = g(z, k)$ gilt. Wir erhalten die diophantische Gleichung zu g wie üblich als Summe der Quadrate der Polynome. □

Lemma 4.16. *Falls $a > y^k$, dann ist $2ay - y^2 - 1 > y^k$.*

Beweis. Setze $g(y) = 2ay - y^2 - 1$. Dann ist wegen $a \geq 2$ schon $g(1) = 2a - 2 \geq a$. Für $1 \leq y < a$ ist $g'(y) = 2a - 2y > 0$, also ist $g(y) \geq a$ für $1 \leq y < a$. Dann ist $2ay - y^2 - 1 \geq a > y^k$ für $a > y^k \geq y$. □

Satz 4.17. *Die Exponentialfunktion $h(n, k) = n^k$ ist diophantisch.*

Beweis. Wir erweitern das System (I-VIII) zu (I-XII) durch:

$$(x - y(a - n) - m)^2 = (f - 1)^2(2an - n^2 - 1)^2 \tag{IX}$$

$$m + g = 2an - n^2 - 1 \tag{X}$$

$$w = n + h = k + l \tag{XI}$$

$$a^2 - (w^2 - 1)(w - 1)^2 z^2 = 1. \tag{XII}$$

Der Satz folgt dann aus:

> ***Behauptung:*** $m = n^k$ genau dann, wenn (I-XII) in den verbleibenden Variablen lösbar ist.
>
> Beweis:
>
> „⇐“: Angenommen, wir haben eine Lösung zu (I-XII). Nach (XI) ist $w > 1$, also ist $(w - 1)z > 0$ und mit (XII) ist $a > 1$. Satz 4.14 liefert $x = x_k(a)$ und $y = y_k(a)$. Mit Lemma 4.12 und (IX) folgt
>
> $$m \equiv n^k \mod 2an - n^2 - 1.$$
>
> Nach (XI) ist $k, n < w$ und mit Lemma 4.8 liefert (XII) $a = x_j(w)$ und $(w - 1)z = y_j(w)$ für ein j. Nach Lemma 4.11 ist $j \equiv 0 \mod w - 1$, sodass gilt $j \geq w - 1$. Dann liefert Lemma 4.13 schon $a \geq w^{w-1} > n^k$. Dann ist nach (X) $m < 2an - n^2 - 1$ und nach Lemma 4.16 $n^k < 2an - n^2 - 1$. Da m und n^k kongruent und kleiner als der Rest $2an - n^2 - 1$ sind, sind sie gleich.
>
> „⇒“: Angenommen, $m = n^k$. Wir zeigen, dass dann das System (I-XII) gilt. Wähle eine beliebige Zahl w, sodass $w > n$ und $w > k$. Setze $a = x_{w-1}(w)$, also ist $a > 1$. Nach Lemma 4.8 ist $y_{w-1}(w) \equiv 0 \mod w - 1$, also kann man $y_{w-1}(w) = z(w - 1)$ schreiben und (XII) gilt. Für $h = w - n$ und $l = w - k$ gilt auch (XI). Erneut ist $a > n^k$, sodass nach Lemma 4.16 $m = n^k < 2an - n^2 - 1$, also auch (X) gilt. Mit $x = x_k(a)$ und $y = y_k(a)$ lässt sich durch Lemma 4.12 ein f definieren, sodass $x - y(a - n) - m = \pm(f - 1)(2an - n^2 - 1)$ gilt, also ist auch (IX) erfüllt. Nach Satz 4.14 finden wir schließlich eine Lösung für (I-VIII).
>
> ■
>
> □

4.3 Folgerungen

Wir haben gesehen, dass die Exponentialfunktion diophantisch ist. Dadurch können wir für weitere Funktionen zeigen, dass sie diophantisch sind.

Beispiel 4.18. $h(u,v,w) = u^{v^w}$ ist diophantisch.

Beweis. Wir zeigen, dass man h als diophantischen Ausdruck schreiben kann.
Betrachte $y = u^{v^w} \Leftrightarrow \exists z(y = u^z \wedge z = v^w)$.
Nach Satz 4.17 gibt es ein Polynom P, sodass gilt:

$$y = u^z \Leftrightarrow \exists r_1, \ldots, r_n[P(y,u,z,r_1,\ldots,r_n) = 0],$$
$$y = v^w \Leftrightarrow \exists s_1, \ldots, s_n[P(z,v,w,s_1,\ldots,s_n) = 0].$$

Nach Bemerkung 3.4 ist:

$$y = u^{v^w} \Leftrightarrow \exists z, r_1, \ldots, r_n, s_1, \ldots, s_n[P^2(y,u,z,r_1,\ldots,r_n) + P^2(z,v,w,s_1,\ldots,s_n) = 0].$$

□

Bemerkung 4.19. Wir haben bereits gesehen, dass diophantische Ausdrücke, die durch ein logisches *und* ($\wedge$) verbunden sind, mithilfe des Satzes von Lagrange verkürzt werden können. Wir können auch diophantische Ausdrücke, die durch ein logisches *oder* ($\vee$) verbunden sind, auf einen Ausdruck reduzieren, denn es gilt:

$$\begin{aligned}&\exists r_1, \ldots, r_n(P_1 = 0) \vee \exists s_1, \ldots, s_m(P_2 = 0)\\ &\quad \Leftrightarrow \exists r_1, \ldots, r_n, s_1, \ldots, s_m(P_1 \cdot P_2 = 0).\end{aligned}$$

Wir können also zusammenfassen, dass wir in diophantischen Ausdrücken die logischen Operationen *und* ($\wedge$), *oder* ($\vee$) sowie *es existiert* ($\exists$) beliebig verwenden können. Das Ergebnis beschreibt weiterhin eine diophantische Menge. Wir werden in Abschnitt 4.4 sehen, dass wir sogar noch mehr Möglichkeiten haben, diophantische Ausdrücke zu bilden. Wir werden auch bemerken, dass es dennoch Grenzen gibt.

Notation. Für $\alpha \in \mathbb{R}$ bezeichnen wir mit $[\alpha]$ die eindeutige ganze Zahl, für die gilt:

$$[\alpha] \leq \alpha < [\alpha] + 1.$$

Binomialkoeffizient

Wir zeigen, dass der Binomialkoeffizient durch einen diophantischen Ausdruck beschrieben werden kann.

Lemma 4.20. *Für* $0 < k \leq n$ *und* $u > 2^n$ *gilt:* $[(u+1)^n u^{-k}] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$.

Beweis. Wir setzen $S + R := \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = (u+1)^n u^{-k}$, wobei $S := \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$ und $R := \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$.
Dann ist S eine ganze Zahl und es gilt:

$$\begin{aligned}R &< u^{-1} \sum_{i=0}^{k-1} \binom{n}{i}\\ &< u^{-1} \sum_{i=0}^{n} \binom{n}{i}\\ &= u^{-1}(1+1)^n\\ &< 1.\end{aligned}$$

Also ist $S \leq (u+1)^n u^{-k} < S + 1$. □

Lemma 4.21. *Für $0 < k \leq n$ und $u > 2^n$ gilt:* $[(u+1)^n u^{-k}] \equiv \binom{n}{k} \mod u$.

Beweis. In Lemma 4.20 sind alle Summanden für $i > k$ durch u teilbar. □

Proposition 4.22. *$f(n,k) = \binom{n}{k}$ ist diophantisch.*

Beweis. Wegen $\binom{n}{k} \leq \sum_{i=0}^{n} \binom{n}{i} = 2^n < u$ ist nach Lemma 4.21 der Binomialkoeffizient $\binom{n}{k}$ die eindeutige positive ganze Zahl, die kleiner als u und kongruent zu $[(u+q)^n u^{-k}]$ modulo u ist.
Also gilt:

$$z = \binom{n}{k} \Leftrightarrow \exists u, v, w (v = 2^n \wedge u > v \wedge w = [(u+1)^n u^{-k}] \wedge z \equiv w \mod u \wedge z < u).$$

Nach Bemerkung 4.19 genügt es zu bemerken, dass alle durch $\wedge$ getrennten Ausdrücke diophantisch sind, um zu sehen, dass der gesamte Ausdruck diophantisch ist. Der Ausdruck $v = 2^n$ ist nach Satz 4.17 diophantisch. Die Ungleichung $u > v$ ist diophantisch nach Beispiel 3.3 iii).
Es gilt:

$$w = [(u+1)^n u^{-k}] \Longleftrightarrow \exists x, y, t (t = u+1 \wedge x = t^n \wedge y = u^k \wedge w \leq xy^{-1} < w+1),$$

also ist auch dieser Ausdruck diophantisch.
Schließlich ist auch der letzte Ausdruck diophantisch, denn es gilt:

$$z \equiv w \mod u \wedge z < u \Longleftrightarrow \exists x, y (w = z + (x-1)u \wedge u = z + y).$$

□

Fakultät

Wir zeigen mithilfe des Binomialkoeffizienten, dass die Fakultät durch einen diophantischen Ausdruck beschrieben werden kann.

Lemma 4.23. *Falls $r > (2x)^{x+1}$ gilt, dann ist $x! = \left[r^x \binom{r}{x}^{-1}\right]$.*

Beweis. Sei $r > (2x)^{x+1}$, dann ist

$$\begin{aligned} r^x \binom{r}{x}^{-1} &= \frac{r^x x!}{r(r-1)\cdots(r-x+1)} \\ &= x! \left(\frac{1}{(1-\frac{1}{r})} \cdots \left(1 - \frac{x-1}{r}\right)\right) \\ &< x! \cdot \left(\frac{1}{1-\frac{x}{r}}\right)^x. \end{aligned}$$

Also gilt

$$\begin{aligned}\frac{1}{1-\frac{x}{r}} &= 1+\frac{x}{r}+\left(\frac{x}{r}\right)^2+\cdots \\ &= 1+\frac{x}{r}\left(1+\frac{x}{r}+\left(\frac{x}{r}\right)^2+\cdots\right) \\ &< 1+\frac{x}{r}\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right) \\ &= 1+\frac{2x}{r}\end{aligned}$$

und

$$\begin{aligned}\left(1+\frac{2x}{r}\right)^x &= \sum_{j=0}^{x}\binom{x}{j}\left(\frac{2x}{r}\right)^j \\ &< 1+\frac{2x}{r}\sum_{j=1}^{x}\binom{x}{j} \\ &< 1+\frac{2x}{r}\cdot 2x,\end{aligned}$$

also

$$\begin{aligned}r^x\binom{r}{x}^{-1} &< x!+\frac{2x}{r}\cdot x!2^x \\ &< x!\frac{2^{x+1}x^{x+1}}{r} \\ &< x!+1.\end{aligned}$$

□

Proposition 4.24. *$g(n) = n!$ ist diophantisch.*

Beweis. Es gilt:

$$\begin{aligned}m = n! \Longleftrightarrow \exists r,s,t,u,v(&s = 2x+1 \wedge t = x+1 \wedge r = s^t \\ &\wedge u = r^n \wedge v = \binom{r}{n} \wedge mv \le u < (m+1)v).\end{aligned}$$

□

Das Produkt $\prod_{k-1}^{y}(a+bk)$
Wir zeigen mithilfe des Binomialkoeffizienten und mithilfe der Fakultät, dass das Produkt $\prod_{k-1}^{y}(a+bk)$ durch einen diophantischen Ausdruck beschrieben werden kann.

Lemma 4.25. *Sei $bq \equiv a \mod M$, dann ist $\prod_{k=1}^{y}(a+bk) \equiv b^y y!\binom{q+y}{y} \mod M$.*

Beweis. Es gilt

$$\begin{aligned} b^y y!\binom{q+y}{y} &= b^y(q+y)(q+y-1)\cdots(q+1) \\ &= (bq+yb)(bq+(y-1)b)\cdots(bq+b) \\ &\equiv (a+yb)(a+(y-1)b)\cdots(a+b) \mod M. \end{aligned}$$

□

Proposition 4.26. *$h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ ist diophantisch.*

Beweis. Wähle in Lemma 4.25 wie vorher $M = b(a+by)^y + 1$. Dann ist $\mathrm{ggT}(M,b) = 1$ und $M > \prod_{k=1}^{y}(a+bk)$. Daher ist die Kongruenz $bq \equiv a \mod M$ für q lösbar. Dann ist $\prod_{k=1}^{y}(a+bk)$ die eindeutige Zahl, die kleiner als M und kongruent zu $b^y y!\binom{q+y}{y}$ modulo M ist, d. h.

$$\begin{aligned} z = \prod_{k=1}^{y}(a+bk) \Longleftrightarrow \exists M,p,q,r,s,t,u,v,w,x\ [&r = a+by \wedge s = r^y \wedge M = bs+1 \\ &\wedge bq = a+Mt \wedge u = b^y \wedge v = y! \wedge z < M \\ &\wedge w = q+y \wedge x = \binom{w}{y} \wedge z+Mp = uvx]. \end{aligned}$$

Mithilfe der Ausdrücke, die wir für die Exponentialfunktion, die Fakultät und den Binomialkoeffizienten entwickelt haben, folgt die Proposition. □

4.4 Gebundene Quantoren und Grenzen Diophantischer Ausdrücke

Wir haben nun einige Beispiele diophantischer Funktionen und Ausdrücke gesehen. Dabei erlaubt die Sprache der diophantischen Ausdrücke die Verwendung der logischen Operatoren $\wedge$, $\vee$ und $\exists$. In diesem Abschnitt werden wir sehen, dass diophantische Ausdrücke sogar noch weitreichender sind als uns bisher bewusst ist.

Definition 4.27. Der *gebundene Existenzquantor* $(\exists y)_{\leq x}\ldots$ wird definiert als

$$(\exists y)(y \leq x) \wedge \ldots),$$

der *gebundene Allquantor* $(\forall y)_{\leq x}\ldots$ wird definiert als

$$(\forall y)(y > x \vee \ldots).$$

Wir werden zeigen, dass gebundene Quantoren mit diophantischen Ausdrücken verträglich sind. Danach sehen wir, dass diophantische Ausdrücke mit der Negation $\neg$, der Implikation $\Rightarrow$ und dem ungebundenen Allquantor $\forall$ nicht verträglich sind.

Lemma 4.28. *Es gilt:*

$$\begin{aligned}&(\forall k)_{\leq y}(\exists y_1, \ldots, y_m)[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\\ \Longleftrightarrow &\exists u(\forall k)_{\leq y}(\exists y_1, \ldots, y_m)_{\leq u}[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0].\end{aligned}$$

Beweis.

„$\Leftarrow$“: klar.

„$\Rightarrow$“: Angenommen, die linke Aussage gilt für gegebene $y, x_1, \ldots, x_n$. Dann gibt es eindeutige Zahlen $y_1^{(k)}, \ldots, y_m^{(k)}$ für $k = 1, 2, \ldots, y$ mit

$$P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) = 0.$$

Wählen wir u als das Maximum dieser Zahlen, also

$$u := \max\{y_j^{(k)} \,:\, j = 1, \ldots, m; k = 1, \ldots, y\},$$

dann folgt sofort die rechte Seite.

□

Lemma 4.29. *Sei $Q(y, u, x_1, \ldots, x_n)$ ein Polynom mit den Eigenschaften*

(1) $Q(y, u, x_1, \ldots, x_n) > u$, *(2)* $Q(y, u, x_1, \ldots, x_n) > y$,

(3) $k \leq y$ *und* $y_1, \ldots, y_m \leq u \Rightarrow |P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)| \leq Q(y, u, x_1, \ldots, x_n)$.

Dann gilt:

$$\begin{aligned}&(\forall k)_{\leq y}(\exists y_1, \ldots, y_m)[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\\ \Longleftrightarrow &\exists c, t, a_1, \ldots, a_m(1 + ct = \prod_{k=1}^{y}(1 + kt)) \wedge t = Q(y, u, x_1, \ldots, x_n)!\\ &\wedge (1 + ct) \mid \prod_{j=1}^{u}(a_1 - j) \wedge \cdots \wedge (1 + ct) \mid \prod_{j=1}^{u}(a_m - j)\\ &\wedge P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \mod 1 + ct).\end{aligned}$$

Wir bemerken, dass die „kompliziertere“ rechte Seite der Äquivalenz keine gebundenen Allquantoren enthält. Dadurch ist die rechte Seite also weniger kompliziert als die linke Seite.

Beweis.

„$\Leftarrow$“: Für jedes $k = 1, \ldots, y$ sei p_k ein Primfaktor von $1 + kt$. Sei $y_i^{(k)}$ der Rest der Division von $a_i, i = 1, \ldots, m$ geteilt durch p_k.

Behauptung: Für jedes k und i gilt:

(a) $1 \leq y_i^{(k)} \leq u$,

(b) $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)})$.

Beweis:

(a): Es gilt $p_k \mid kt$, $1+kt \mid 1+ct$ und $1+ct \mid \prod_{j=1}^{u}(a_i-j)$. Also gilt $p_k \mid \prod_{j=1}^{u}(a_i-j)$. Da p_k eine Primzahl ist, gilt $p_k \mid a_i - j$ für ein $j = 1, \ldots, u$, also ist

$$j \equiv a_i \equiv y_i^{(k)} \mod p_k.$$

(b): Wir bemerken, dass gilt

$$1 + ct \equiv 1 + kt \equiv 0 \mod p_k,$$

also auch

$$k + kct \equiv c + kct \mod p_k$$

und damit

$$k \equiv c \mod p_k.$$

Aus (a) haben wir

$$y_i^{(k)} \equiv a_i \mod p_k$$

und damit erhalten wir

$$P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_n^{(k)}) \equiv P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \mod p_k.$$

Schließlich ist

$$|P(y, k, x_1, \ldots, x_n, y_1^{(k))}, \ldots, y_m^{(k)})| \leq Q(y, u, x_1, \ldots, x_n) < p_k.$$

■

Aus der Behauptung folgt „⇐“.

„⇒“: Sei $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) = 0$ für jedes $k = 1, \ldots, t$ mit $y_j^{(k)}$. Setze $t = Q(y, u, x_1, \ldots, x_n)!$ und wegen $\prod_{k=1}^{y}(1 + kt) \equiv 1 \mod t$ finden wir ein c mit

$$1 + ct = \prod_{k=1}^{y}(1 + kt).$$

Dann ist für $1 \leq k < l \leq y$

$$\text{ggT}(1 + kt, 1 + lt) = 1.$$

Sei p so, dass $p \mid 1 + kt$ und $p \mid 1 + lt$ gilt, dann ist $p \mid l - k$, also $p < y$. Wegen $Q(y, u, x_1, \ldots, x_n) > y$ gelte dann $p \mid t$, was unmöglich ist. Daher sind die Zahlen $1+kt$ für $k = 1, \ldots, t$ paarweise teilerfremd. Dann liefert uns der Chinesische Restsatz eine Zahl a_i für alle $1 \leq i \leq m$, sodass gilt

$$a_i \equiv y_i^{(k)} \mod 1 + kt \text{ für } k = 1, \ldots, y.$$

Wie oben gilt $k \equiv c \mod 1 + kt$, also gilt

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) \mod 1 + kt = 0.$$

Damit gilt auch

$$a_i \equiv y_i^{(k)} \mod 1 + kt,$$

also erhalten wir

$$1 + kt \mid a_i - y_i^{(k)}.$$

Wegen $1 \leq y_i^{(k)} \leq u$ ist

$$1 + lkt \mid \prod_{j=1}^{u} (a_i - j)$$

und weil die $1 + kt$ paarweise teilerfremd sind, gilt schließlich

$$1 + ct \mid \prod_{j=1}^{u} (a_i - j).$$

□

Satz 4.30. *Für ein Polynom P sind die Mengen*

$$R = \{\langle y, x_1, \ldots, x_n\rangle | (\exists z)_{\leq y} (\exists y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$
$$S = \{\langle y, x_1, \ldots, x_n\rangle | (\forall z)_{\leq y} (\exists y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$

diophantisch.

Beweis. Wir beweisen den Satz mithilfe von Lemma 4.28 und 4.29. Betrachte

$$P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{r=1}^{N} t_r,$$

wobei jedes t_r die Form

$$t_r = |c| y^a k^b x_1^{q_1} x_2^{q_2} \cdots x_n^{q_n} y_1^{s_1} y_2^{s_2} \cdots y_m^{s_m}$$

für eine ganze Zahl $c \neq 0$ hat. Setze

$$u_r = c y^{a+b} x_1^{q_1} \cdots x_n^{q_n} u^{s_1 + \cdots + s_m}.$$

Wir wählen ein Polynom Q, das die Eigenschaften (1), (2) und (3) aus Lemma 4.29 erfüllt:

$$Q(y, u, x_1, \ldots, x_n) = u + y + \sum_{r=1}^{N} u_r.$$

Offenbar sind die geforderten Eigenschaften erfüllt. Also gilt:

$$\begin{aligned}
&(\forall k)_{\leq y}(\exists y_1,\ldots,y_m)[P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)=0]\\
\Longleftrightarrow&(\exists u,c,t,a_1,\ldots,a_m)[1+ct=\prod_{k=1}^{y}(1+kt)\wedge t=Q(y,u,x_1,\ldots,x_n)!\\
&\wedge 1+ct\mid\prod_{j=1}^{u}(a_1-j)\wedge\cdots\wedge 1+ct\mid\prod_{j=1}^{u}(a_m-j)\\
&\wedge P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)\equiv 0 \mod 1+ct]\\
\Longleftrightarrow&(\exists u,t,a_1,\ldots,a_n,e,f,g_1,\ldots,g_m,h_1,\ldots,h_n,l)[e=1+ct\\
&\wedge e=\prod_{k=1}^{y}(1+kt)\wedge f=Q(y,u,x_1,\ldots,x_n)\wedge t=f!\wedge g_1=a_1-u-1\\
&\wedge\cdots\wedge g_m=a_m-u-1\wedge h_1=\prod_{k=1}^{u}(g_1+k)\wedge\cdots\wedge h_m=\prod_{k=1}^{u}(g_m+k)\\
&\wedge e\mid h_1\wedge\cdots\wedge e\mid h_m\wedge l=P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_n)\wedge e\mid l].
\end{aligned}$$

All diese Ausdrücke sind diophantisch nach den Propositionen 4.22, 4.24 und 4.26.

□

Beispiel 4.31. Mithilfe der entwickelten Methoden können wir weitere Mengen als diophantische Ausdrücke angeben:

i) Die Menge $\mathbb{P}$ der Primzahlen:

$$x\in\mathbb{P}\Longleftrightarrow x>1\wedge(\forall y,z)_{\leq x}[yz<x\vee yz>x\vee y=1\vee z=1].$$

Nach Satz 3.11 gibt es ein Polynom B, sodass genau die positiven ganzen Zahlen, die im Bild von B liegen, die Primzahlen sind. Ein solches Polynom wird in [Mat71] explizit konstruiert.

ii) Die Funktion $g(y)=\prod_{k=1}^{y}(1+k^2)$:

$$\begin{aligned}
&z=g(y)\\
\Longleftrightarrow&\exists u\{S(1,u)=2\wedge(\forall k)_{\leq y}[k=1\\
&\vee(S(k,u)=(1+k^2)S(k-1,u))]\wedge z=S(y,u)\}\\
\Longleftrightarrow&\exists u\{S(1,u)=2\wedge(\forall k)_{\leq y}[k=1\vee\exists a,b,c(a=k-1\\
&\wedge b=S(a,u)\wedge c=S(k,u)\wedge c=(1+k^2)b]\wedge z=S(y,u)\}.
\end{aligned}$$

Wir haben hier mithilfe des Satzes über die Nachfolgerfunktion (3.10) die Folge der $g(i)$ durch einzelne Zahlen u kodiert, sodass

$$S(i,u)=g(i)\text{ für }i=1,\ldots,y$$

gilt.

Definition und Bemerkung 4.32. Jedes Polynom in positiven ganzzahligen Koeffizienten lässt sich aus der Eins, Variablen und wiederholter Addition und Multiplikation konstruieren. Wir fixieren die Variablen $x_0, x_1, x_2, \ldots$ und erzeugen mithilfe der Cantor'schen Paarungsfunktion folgende Aufzählung aller Polynome dieser Art:

$$\begin{aligned} P_1 &= 1 \\ P_{3i-1} &= x_{i-1} \\ P_{3i} &= P_{L(i)} + P_{R(i)} \\ P_{3i+1} &= P_{L(i)} \cdot P_{R(i)}. \end{aligned}$$

Wir schreiben $P_i = P_i(x_0, x_1, \ldots, x_n)$ für n so groß, dass alle auftretenden Variablen enthalten sind (im Allgemeinen wird P_i nicht von all diesen Variablen abhängen). Sei

$$D_n = \{x_0 : (\exists x_1, \ldots, x_n)[P_{L(n)}(x_0, \ldots, x_n) = P_{R(n)}(x_0, \ldots, x_n)]\}.$$

Die Funktionen $P_{L(n)}$ und $P_{R(n)}$ umfassen nicht alle x_i, aber umfassen auf jeden Fall keine anderen Variablen. Nach Konstruktion der Folge der P_i beinhaltet die Folge

$$D_1, D_2, D_3, \ldots$$

alle diophantischen Mengen. Mithilfe dieser Konstruktion können wir die universelle diophantische Menge definieren:

$$U = \{\langle n, x\rangle : x \in D_n\}.$$

Wir bezeichnen U als die *universelle diophantische Menge* und werden später zeigen, dass diese Menge diophantisch ist (Satz 6.1).

Definition 4.33. Wir definieren die Menge

$$V = \{n : n \notin D_n\}.$$

Wir beweisen später, dass V nicht diophantisch ist (Satz 6.2). An dieser Stelle wollen wir anhand dieser Menge zeigen, dass diophantische Ausdrücke unter manchen Operationen nicht abgeschlossen sind.

Lemma 4.34. *Diophantische Ausdrücke sind nicht abgeschlossen unter* $\neg$, $\Rightarrow$ *und* $\forall$.

Beweis. Es gilt:

$$\begin{aligned} x \in V &\iff \neg(\exists z_1, \ldots, z_k)[P(x, x, z_1, \ldots, z_k) = 0] \\ &\iff \{(\exists z_1, \ldots, z_k)[P(x, x, z_1, \ldots, z_k) = 0] \Rightarrow 1 = 0\} \\ &\iff (\forall z_1, \ldots, z_k)[P(x, x, z_1, \ldots, z_k) > 0 \vee P(x, x, z_1, \ldots, z_k) < 0], \end{aligned}$$

wobei P das Polynom ist, das U definiert.

□

5 Rekursive Funktionen

In diesem Kapitel widmen wir uns den rekursiven Funktionen. Wir wollen diesen Begriff definieren und dann kurz darauf eingehen, dass die Klasse der rekursiven Funktionen ein Berechenbarkeitsmodell liefert, das äquivalent zur Turing-Maschine ist. Schließlich zeigen wir, dass eine Funktion genau dann diophantisch ist, wenn sie rekursiv ist.

5.1 Rekursive und diophantische Funktionen

Definition 5.1. Eine Funktion heißt *rekursive Funktion*, falls wir sie aus den Funktionen $c(x) = 1$, $s(x) = x + 1$ und $U_i^n(x_1, \ldots, x_n) = x_i$ für $1 \leq i \leq n$
bilden können. Dazu stehen folgende Operationen zur Verfügung:

- *Komposition:* Wir bilden aus den rekursiven Funktionen $g_1, \ldots, g_m$ und $f(t_1, \ldots, t_m)$ die Funktion

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

- *Primitive Rekursion:* Wir bilden aus den rekursiven Funktionen f und g die Funktion $h(x_1, \ldots, x_n, z)$ durch

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n), \\ h(x_1, \ldots, x_n, t+1) &= g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n). \end{aligned}$$

  Für $n = 0$ ist f konstant. In diesem Fall erhalten wir h direkt aus g.

- *Minimalisierung:* Wir erhalten die Funktion

$$h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)]$$

  aus den rekursiven Funktionen f und g. Dabei sollen sie derart sein, dass für jedes $x_1, \ldots, x_n$ mindestens ein y existiert mit $f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)$. Wir fordern also, dass h überall definiert ist.

Beispiel 5.2. Wir betrachten einige Beispiele rekursiver Funktionen:

(1) Die Nachfolgerfunktion $S(i, u)$ ist rekursiv.

(2) $x + y$ ist rekursiv wegen $x + 1 = s(x)$ und $x + (t + 1) = s(x + t) = g(t, x + t, x)$, wobei $g(u, v, w) = s(U_2^3(u, v, w))$ ist.

(3) $x \cdot y$ ist rekursiv wegen $x \cdot 1 = U_1^1(x)$ und $x \cdot (t+1) = (x \cdot t) + x = g(t, x \cdot t, x)$, wobei $g(u, v, w) = U_2^3(u, v, w) + U_3^3(u, v, w)$ ist.

(4) Für jedes konstante k ist $c_k(x) = k$ als konstante Funktion rekursiv, denn $c_1(x)$ ist eine der Anfangsfunktionen und $c_{k+1}(x) = c_k(x) + c(x)$.

(5) Jedes Polynom $P(x_1, \ldots, x_n)$ mit positiven ganzzahligen Koeffizienten ist rekursiv, denn jede solche Funktion lässt sich durch endliche Wiederholung von Addition und Multiplikation von Variablen und $c(x)$ beschreiben (beispielsweise ist das Polynom $2x^2y + 3xz^3 + 5 = c_2(x) \cdot x \cdot x \cdot y + c_3(x) \cdot x \cdot z \cdot z \cdot z + c_5(x)$ rekursiv, wobei wir (2), (3), (4) und Komposition benötigen).

Satz 5.3. *Eine Funktion ist genau dann diophantisch, wenn sie rekursiv ist.*

Beweis.

„⇐“: Sei f diophantisch. Wir schreiben

$$\begin{aligned} y = f(x_1, \ldots, x_n) \iff (\exists t_1, \ldots, t_m)[&P(x_1, \ldots, x_n, y, t_1, \ldots, t_m) \\ &= Q(x_1, \ldots, x_n, y, t_1, \ldots, t_m)] \end{aligned}$$

für Polynome P, Q in positiven ganzzahligen Koeffizienten. Nach dem Satz über die Nachfolgerfunktion (3.10) gilt dann:

$$\begin{aligned} f(x_1, \ldots, x_n) = S(1, \min_u[&P(x_1, \ldots, x_n, S(1,u), \ldots, S(m+1,u)) \\ &= Q(x_1, \ldots, x_n, S(1,u), \ldots, S(m+1,u))]). \end{aligned}$$

f ist rekursiv, denn P, Q und die Nachfolgerfunktion sind rekursiv.

„⇒“: Wir zeigen, dass diophantische Funktionen unter den Operationen Komposition, Primitive Rekursion und Minimalisierung abgeschlossen sind. Aus der Definition folgt sofort, dass die Anfangsfunktionen sowie die Nachfolgerfunktion diophantisch sind.

Komposition:

Falls $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots g_n(x_1, \ldots, x_n))$ für die diophantischen Funktionen $f, g_1 \ldots, g_m$ gilt, so ist auch h diophantisch wegen:

$$\begin{aligned} & y = h(x_1, \ldots, x_n) \\ \iff & (\exists t_1, \ldots, t_m)[t_1 = g_1(x_1, \ldots, x_n) \wedge \ldots \\ & \wedge t_m = g_m(x_1, \ldots, x_n) \wedge y = f(t_1, \ldots, t_m)]. \end{aligned}$$

Primitive Rekursion:

Falls

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, t+1) &= g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n) \end{aligned}$$

für die diophantischen Funktionen f und g gilt, dann gilt mit dem Satz über die Nachfolgerfunktion (3.10):

$$\begin{aligned} & y = h(x_1, \ldots, x_n, z) \\ \Longleftrightarrow & (\exists u)\{(\exists v)[v = S(1,u) \wedge v = f(x_1, \ldots, x_n)] \\ & \wedge (\forall t)_{\leq z}[(t = z) \vee (\exists v)(v = S(t+1,u) \\ & \wedge v = g(t, S(t,u), x_1, \ldots, x_n))] \wedge y = S(z,u)\}. \end{aligned}$$

Also ist h nach Satz 4.30 diophantisch. Wir bemerken, dass wir mithilfe des Satzes über die Nachfolgerfunktion (3.10) die Funktionswerte von h kodiert haben.

Minimalisierung:

Falls

$$h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)]$$

für die diophantischen Funktionen f und g, dann ist auch h diophantisch wegen:

$$\begin{aligned} & y = h(x_1, \ldots, x_n) \\ \Longleftrightarrow & \exists z[z = f(x_1, \ldots, x_n, y) \wedge z = g(x_1, \ldots, x_n, y)] \\ & \wedge (\forall t)_{\leq y}[(t = y) \vee (\exists u, v)(u = f(x_1, \ldots, x_n, t) \\ & \wedge v = g(x_1, \ldots, x_n, t) \wedge (u < v \vee v < u)]. \end{aligned}$$

Also sind diophantische Funktionen abgeschlossen unter Komposition, Primitiver Rekursion und Minimalisierung.

□

5.2 Rekursive Funktionen und Turingmaschinen

Die rekursiven Funktionen bilden ein Berechenbarkeitsmodell, das äquivalent zu Turingmaschinen ist. Jede rekursive Funktion ist also turing-berechenbar und umgekehrt.
In [LP98] finden wir einen formalen Beweis für die Äquivalenz. Dabei wird keine deterministische Turingmaschine verwendet, sondern eine sogenannte Random Access Turingmaschine. Nach [LP98, Theorem 4.4.2] sind jedoch beide Varianten äquivalent.
Nach [LP98, Theorem 4.7.1] sind Funktionen genau dann rekursiv, wenn sie turing-berechenbar sind. Im Beweis wird gezeigt, dass rekursive Funktionen turing-berechenbar sind. Für die Rückrichtung wird eine rekursive Funktion zu einer Turingmaschine konstruiert.

6 Negative Lösung zu H10

Nach dem vorherigen Abschnitt lässt sich jedes durch Turingmaschinen entscheidbare Problem auch mithilfe von rekursiven Funktionen entscheiden und umgekehrt. Weiterhin ist wohlbekannt, dass es Probleme gibt, die nicht von Turing-Maschinen entschieden werden können, beispielsweise das Halteproblem (vgl. [Sip06, Kap. 4.2]). Entsprechend gibt es auch keine rekursive Funktion, die das Halteproblem beschreibt. Wenn wir zeigen, dass die Lösbarkeit diophantischer Gleichungen nicht durch eine rekursive Funktion beschrieben werden kann, folgt wegen der Äquivalenz der Berechenbarkeitsmodelle sofort, dass dieses Problem auch nicht von einer Turing-Maschine entschieden werden kann.

In diesem Kapitel wollen wir beweisen, dass die Lösbarkeit diophantischer Gleichungen unentscheidbar ist. Dazu betrachten wir die universelle diophantische Menge U aus Definition und Bemerkung 4.32 und die nicht-diophantische Menge V aus Definition 4.33 und konstruieren eine nicht-rekursive Funktion. Damit zeigen wir dann per Widerspruch, dass es keinen Algorithmus zur Entscheidung diophantischer Gleichungen gibt. Schließlich zeigen wir, dass eine Menge genau dann diophantisch ist, wenn sie rekursiv aufzählbar ist. Damit beantworten wir die natürliche Frage, welche Mengen diophantisch sind.

6.1 Universelle diophantische Menge und nicht-rekursive Funktion

Wir betrachten $D_n = \{x_0 : (\exists x_1, \ldots, x_n)[P_{L(n)}(x_0, \ldots, x_n) = P_{R(n)}(x_0, \ldots, x_n)]\}$ und $U = \{\langle n, x\rangle : x \in D_n\}$ aus Definition und Bemerkung 4.32.

Satz 6.1. *Die Menge U ist diophantisch.*

Beweis. Nach dem Satz über die Nachfolgerfunktion (3.10) ist

$$\begin{aligned}
&\exists u\{S(1,u) = 1 \wedge S(2,u) = x \\
&\wedge (\forall i)_{\leq n}[S(3i,u) = S(L(i),u) + S(R(i),u)] \\
&\wedge (\forall i)_{\leq n}[S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)] \\
&\wedge S(L(n),u) = S(R(n),u)\} \qquad\qquad =: X_n.
\end{aligned}$$

ein diophantischer Ausdruck. Wir zeigen, dass dieser Ausdruck zu $x \in D_n$ äquivalent ist.

Behauptung: $x \in D_n \iff x \in X_n$.
Beweis:

„$\Rightarrow$“: Sei also $x \in D_n$ für ein gegebenes x und n. Dann gibt es Zahlen $t_1, \ldots, t_n \in \mathbb{N}^+$ mit $P_{L(n)}(x, t_1, \ldots, t_n) = Q_{L(n)}(x, t_1, \ldots, t_n)$. Nach dem Satz über die Nachfolgerfunktion (3.10) können wir ein u wählen, sodass gilt:

$$S(j,u) = P_j(x, t_1, \ldots, t_n) = Q_j(x, t_1, \ldots, t_n) \text{ für } j = 1, \ldots, 3n+2. \qquad (*)$$

Dann gilt insbesondere

$$S(2,u) = x \text{ und } S(3i-1,u) = t_{i-1} \text{ für } i = 2,\ldots,n+1$$

und damit

$$x \in X_n.$$

„⇐“: Sei also $x \in X_n$ für ein gegebenes x und n. Sei

$$t_1 = S(5,u),\ \ t_2 = S(8,u),\ \ \ldots,\ \ t_n = S(3n+2,u).$$

Dann gilt schon $(*)$ und wegen

$$S(L(n),u) = S(R(n),u)$$

erhalten wir

$$P_{L(n)}(x,t_1,\ldots,t_n) = P_{R(n)}(x,t_1,\ldots,t_n),$$

also gilt

$$x \in D_n.$$

■
□

Satz 6.2. *Die Menge $V = \{n : n \notin D_n\}$ ist nicht diophantisch.*

Beweis. Wir verwenden Cantors Diagonalargument:
Falls V diophantisch wäre, so gelte $V = D_i$ für ein festes i. Dann folgt:

$$i \in V \iff i \in D_i \text{ und } i \in V \iff i \notin D_i,$$

ein Widerspruch. □

Satz 6.3. *Die Funktion $g(n,x)$, definiert durch*

$$g(n,x) = \begin{cases} 1, & \textit{falls } x \notin D_n \\ 2, & \textit{falls } x \in D_n \end{cases},$$

ist nicht rekursiv.

Beweis. Angenommen, $g(n,x)$ ist rekursiv. Dann ist g diophantisch nach Satz 5.3, also gilt:

$$y = g(n,x) \iff (\exists y_1,\ldots,y_m)[P(n,x,y,y_1,\ldots,y_m) = 0].$$

Dann folgt

$$V = \{x : (\exists y_1,\ldots,y_m)[P(x,x,1,y_1,\ldots,y_m) = 0\},$$

sodass V eine diophantische Menge ist, im Widerspruch zu Satz 6.2.

□

6.2 Die Lösbarkeit diophantischer Gleichungen ist unentscheidbar

Satz 6.4. *Die Lösbarkeit diophantischer Gleichungen ist unentscheidbar.*

Beweis. Nach Satz 6.1 gilt:

$$x \in D_n \iff (\exists z_1, \ldots, z_k)[P(n, x, z_1, \ldots, z_k) = 0],$$

für ein bestimmtes, aber kompliziertes Polynom P. Angenommen, wir haben einen Algorithmus, um die Lösbarkeit diophantischer Gleichungen zu entscheiden. Dieser Algorithmus prüft für ein gegebenes x und n, ob die Gleichung

$$P(n, x, z_1, \ldots, z_k) = 0$$

eine Lösung hat, also, ob $x \in D_n$ gilt. Demnach berechnet dieser Algorithmus die Funktion $g(n, k)$ aus Satz 6.3. Damit ist $g(n, k)$ rekursiv, im Widerspruch zu Satz 6.3. Es gibt also keinen Algorithmus, der die Lösbarkeit diophantischer Gleichungen entscheidet und dieses Problem ist unentscheidbar. □

6.3 Entscheidbare, rekursiv aufzählbare und diophantische Mengen

In diesem Abschnitt gehen wir auf die Zusammenhänge zwischen rekursiv aufzählbaren und diophantischen Mengen ein.

Definition 6.5. (Rekursiv aufzählbare Menge) Eine Menge S von n-Tupeln positiver ganzer Zahlen heißt *rekursiv aufzählbar*, wenn es rekursive Funktionen $f(x, x_1, \ldots, x_n)$ und $g(x, x_1, \ldots, x_n)$ gibt mit

$$S = \{\langle x_1, \ldots, x_n\rangle \,:\, \exists x[f(x, x_1, \ldots, x_n) = g(x, x_1, \ldots, x_n)]\}.$$

Diese Definition ist äquivalent zu Definition 2.1.
Wir nennen eine Menge *entscheidbar* (in Anlehnung an Definition 2.3), wenn ein Algorithmus (oder eine Turingmaschine) existiert, der für eine gegebene Zahl entscheidet, ob sie Element der Menge ist.

Bemerkung 6.6. Jede entscheidbare Menge ist offenbar auch rekursiv aufzählbar. Die Umkehrung gilt im Allgemeinen nicht, denn nach dem Halteproblem gibt es unentscheidbare Mengen, die rekursiv aufzählbar sind.

Satz 6.7. *Eine Menge S ist genau dann diophantisch, wenn sie rekursiv aufzählbar ist.*

Beweis.

„⇒“: Sei S diophantisch. Also gibt es Polynome P und Q mit ganzzahligen Koeffizienten, sodass gilt:

$$\begin{aligned}
&\langle x_1, \ldots, x_n\rangle \in S \\
\iff &\exists y_1, \ldots, y_m[P(x_1, \ldots, x_n, y_1, \ldots, y_m) = Q(x_1, \ldots, x_n, y_1, \ldots, y_m)] \\
\iff &\exists u[P(x_1, \ldots, x_n, S(1, u), \ldots, S(m, u)) = Q(x_1, \ldots, x_n, S(1, u), \ldots, S(m, u))],
\end{aligned}$$

also ist S rekursiv aufzählbar.

„$\Leftarrow$“: Sei S rekursiv aufzählbar. Also gibt es rekursive Funktionen $f(x, x_1, \ldots, x_n)$ und $g(x, x_1, \ldots, x_n)$, sodass gilt:

$$\begin{aligned} & \langle x_1, \ldots, x_n \rangle \in S \\ \Longleftrightarrow & \exists x[f(x, x_1, \ldots, x_n) = g(x, x_1, \ldots, x_n)] \\ \Longleftrightarrow & \exists x, z[z = f(x, x_1, \ldots, x_n) \wedge z = g(x, x_1, \ldots, x_n)]. \end{aligned}$$

Dieser Ausdruck ist nach Satz 5.3 diophantisch.

□

7 Formulierung bekannter Probleme als diophantische Mengen

Wir haben uns nun eingehend mit diophantischen Mengen beschäftigt und in Abschnitt 6.2 gesehen, dass diophantische Mengen nicht entscheidbar sind. In diesem Kapitel möchten wir größere Beispiele diophantischer Mengen betrachten. Entgegen der bisherigen Beispiele möchten wir nun auf wohlbekannte Probleme und Fragen eingehen und diese als diophantische Menge beschreiben.
Wir werden die Vorgehensweise nur skizzieren und verweisen für weitere Details auf die Literatur ([DMR76, Kap. 2, S. 331 ff.]).

7.1 Der Große Fermat

Als den Großen Fermat (oder den Großen Fermatschen Satz) bezeichnet man eine Vermutung, die Pierre de Fermat[1] im 17. Jahrhundert formuliert hat und erst im Jahr 1994 von Andrew Wiles und Richard Taylor[2] bewiesen wurde. Sie besagt, dass für eine natürliche Zahl n größer als 2 die n-te Potenz jeder natürlichen Zahl ungleich Null nicht in die Summe zweier n-Potenzen natürlicher Zahlen ungleich Null zerlegt werden kann.
Demnach hat also die Gleichung

$$x^n + y^n = z^n \tag{F1}$$

für $x, y, z, n \in \mathbb{N}_+$ für $n \geq 3$ keine Lösung.
Eine positive Lösung des 10. Hilbertschen Problems hätte es uns ermöglicht, diese Vermutung für jedes $n > 2$ zu lösen. Wir können sogar die Vermutung als Ganzes als diophantische Menge beschreiben, sodass eine positive Lösung sofort eine Bestätigung oder eine Verneinung geliefert hätte. Wir konstruieren nun die diophantische Menge, die den Großen Fermatschen Satz beschreibt.
Nach Satz 4.17 können wir die Exponentialfunktion als diophantischen Ausdruck angeben. Also gibt es ein Polynom A, sodass

$$A(x, y, z, y_1, \ldots, y_m) = 0$$

genau dann gilt, wenn

$$x = y^z$$

gilt. Daher ist (F1) für die Werte von n lösbar, für die

$$A(p, x, n, x_1, \ldots, x_m)^2 + A(q, y, n, y_1, \ldots, y_m)^2 = A(p + q, z, n, z_1, \ldots, z_n) = 0 \tag{F2}$$

[1] Pierre de Fermat (⋆ca. 1607, †1665) war ein französischer Mathematiker und Jurist, der vor allem für seine Arbeit in der Zahlentheorie bekannt ist.
[2] Der große Fermatsche Satz wurde erst nach über 350 Jahren mit Beweisversuchen vieler bedeutender Mathematiker im Jahr 1994 von Andrew Wiles und Richard Taylor bewiesen.

Lösungen besitzt. Eine äquivalente Formulierung für den Großen Fermat ist dann die Behauptung, dass die diophantische Gleichung

$$A(p, x+1, n+3, x_1, \ldots, x_m)^2 + A(q, y+1, n+3, y_1, \ldots, y_m)^2 + A(p+q, z, n+3, z_1, \ldots, z_m) = 0$$

keine Lösung über $\mathbb{N}$ hat. Damit könnten wir die Vermutung für alle $n > 2$ in einem Schritt durch einen hypothetischen Algorithmus, der diophantische Mengen entscheidet, zeigen. Die Gleichung (F2) kann man explizit angeben, vergleiche dazu [MR75], wo ein solches System diophantischer Gleichungen konstruiert wird.

7.2 Die Goldbach-Vermutung

Ein schwierigeres Beispiel einer diophantischen Menge liefert die Goldbach-Vermutung. Diese Vermutung ist Hilberts 8. Problem und bis heute ungelöst. Sie besagt, dass jede gerade Zahl größer als 2 die Summe zweier Primzahlen ist.

Erneut möchten wir eine diophantische Gleichung konstruieren, die das Problem beschreibt:
Die Gleichung

$$B(p, y_1, \ldots, y_m) = 0 \tag{G1}$$

ist in den Variablen $y_1, \ldots, y_m$ genau dann lösbar, wenn p prim ist (vgl. Beispiel 4.31 i)).
Die Gleichung

$$(u+1)(1 - B(p_1, y_1, \ldots, y_m)^2 - B(p_2, y_1', \ldots, y_m')^2 - (2n + 4 - p_1 - p_2)^2 - t) = a \tag{G2}$$

ist lösbar für alle nicht-positiven a (mit $u = 0$, $t = -a$, $p_1 = p_2 = 2$ und Werten für $y_1, \ldots, y_m, y_1', \ldots, y_m'$ wie in (G1) mit $p = 2$), sowie für genau die positiven a, für die $2a+2$ die Summe zweier Primzahlen ist (mit $u = a-1$, $t = 0$, $p_1+p_2 = 2a+2$ und Werten für $y_1, \ldots, y_m$ wie in (G1) für $p = p_1$ und Werten für $y_1', \ldots, y_m'$ wie in (G1) für $p = p_2$).
Wir können also die Goldbach-Vermutung als die Behauptung schreiben, dass die linke Seite von (G2) jede ganze Zahl repräsentiert, falls die y_i nicht-negativ sind. Wir ersetzen die Variablen durch die Summe der Quadrate vierer neuer Variablen (nach Satz 3.8) und erhalten ein Polynom, dass jede ganze Zahl genau dann repräsentiert, wenn die Goldbach-Vermutung zutrifft. Dadurch haben wir die Vermutung auf diophantische Gleichungen reduziert, aber bisher betrachten wir für jede ganze Zahl eine eigene Gleichung, also ein unendliches System diophantischer Gleichungen. Dieses möchten wir auf eine einzelne Gleichung reduzieren:

Bemerkung. Falls wir einen Algorithmus haben, der in endlich vielen Schritten prüfen kann, ob eine beliebige natürliche Zahl n eine bestimmte Eigenschaft P besitzt (wir sagen dann, dass $P(n)$ gilt), so können wir die Behauptung, dass alle natürlichen Zahlen die Eigenschaft P haben auf die Unlösbarkeit einer bestimmten diophantischen Gleichung reduzieren.
Der Algorithmus liefert uns mit Satz 3.11 die Polynome R und S mit

$$\begin{aligned} P(n) &\iff \exists y_1, \ldots, y_m (R(y_1, \ldots, y_m) = n), \\ \neg P(n) &\iff \exists z_1, \ldots, z_k (S(z_1, \ldots, z_k) = n). \end{aligned}$$

Wir können das betrachtete Polynom auf die Behauptung reduzieren, dass die Gleichung

$$R(y_1, \ldots, y_m) = n$$

für jede natürliche Zahl n lösbar ist oder auf die Behauptung, dass die Gleichung

$$S(z_1, \ldots, z_k) = z_0$$

überhaupt keine Lösungen hat.

Man kann leicht einen Algorithmus angeben, mit dem wir prüfen können, ob $2n + 4$ die Summe zweier Primzahlen ist. Damit lässt sich die Vermutung nicht nur als (G2) formulieren, sondern auch als Behauptung, dass eine bestimmte diophantische Gleichung unlösbar ist. Mithilfe einer positiven Lösung von Hilberts 10. Problem wären wir in der Lage, die Goldbach-Vermutung zu beantworten.

7.3 Primzahlzwillingsvermutung

Wir haben gesehen, dass sich zumindest einige bekannte Probleme auf die Unlösbarkeit diophantischer Gleichungen reduzieren lassen. Wir können aber nicht jedes Problem so umformulieren. Wir betrachten die Primzahlzwillingsvermutung. Diese besagt, dass es unendlich viele Primzahlzwillinge gibt, also Paare von Primzahlen, deren Abstand 2 beträgt. Diese Vermutung lässt sich auch formulieren als

$$\forall n[\exists p(p > n \wedge p \text{ ist prim} \wedge p + 2 \text{ ist prim})]. \tag{Z1}$$

Nun ist die Menge der natürlichen Zahlen n, die (Z1) erfüllen, offenbar eine berechenbare Menge. Sie ist entweder die Menge aller natürlichen Zahlen $\mathbb{N}$ oder eine endliche Teilmenge davon. Da wir allerdings nicht wissen, was von beidem zutrifft, können wir keinen Algorithmus angeben, der n auf diese Eigenschaft überprüft. Dadurch können wir die Primzahlzwillingsvermutung nicht auf die Unlösbarkeit einer bestimmten diophantischen Gleichung reduzieren.

Betrachten wir allerdings eine stärkere Variante, nämlich

$$\forall n[\exists p(n + 4 < p < 2^{n+4} \wedge p \text{ ist prim} \wedge p + 2 \text{ ist prim})], \tag{Z2}$$

so können wir prüfen, ob ein n die Eigenschaft (Z2) erfüllt. Also können wir diese stärkere Variante auf die Unlösbarkeit einer diophantischen Gleichung reduzieren.

Zahlentheoretiker gehen im Übrigen davon aus, dass beide Varianten der Vermutung, also (Z1) und (Z2) wahr sind.

7.4 Motivation für Transformationen in diophantische Mengen

Nachdem wir anhand verschiedener Beispiele gesehen haben, wie man bekannte Probleme in diophantischen Mengen ausdrückt, stellt sich natürlich die Frage, welchen Nutzen das für uns hat.

Auf diese Weise können wir überraschende und unerwartete Verbindungen zwischen verschiedenen mathematischen Bereichen entdecken. Dabei gilt es, diese Verbindungen möglichst sinnvoll auszunutzen.
So können wir versuchen, Kriterien zu finden, die die Unlösbarkeit diophantischer Gleichungen hinreichend implizieren. Bestenfalls lassen sich diese Kriterien leicht und möglicherweise mithilfe von Computern für betrachtete diophantische Gleichungen prüfen.
Womöglich können wir auch eine Klassifikation diophantischer Gleichungen und Definitionen vornehmen, sodass die Übersetzung bekannter Probleme in diophantische Gleichung bestimmten Typs zusätzliche Informationen liefert. Denn die Übersetzung eines Theorems passender Form zeigt, dass die zugehörige diophantische Gleichung keine Lösungen besitzt. Daher lässt sich mit allen Methoden, die im Beweis des Theorems nützlich waren, auch zeigen, dass eine bestimmte diophantische Gleichung keine Lösung hat. Möglicherweise lässt sich mit diesen Methoden die Unlösbarkeit eines bestimmten Typs diophantischer Gleichungen zeigen, sodass wir nützliche Erkenntnisse für bestimmte Gleichungen erhalten. Auf diese Weise könnten alle mathematischen Methoden auch Methoden in der Theorie der diophantischen Gleichungen sein. Das Ziel muss sein, diese Methoden sinnvoll zu nutzen.

8 Ausblick

Wir haben die Entscheidung der Lösbarkeit diophantischer Gleichungen in ganzen Zahlen betrachtet und es stellt sich heraus, dass dieses Problem nicht entscheidbar ist. Natürlich stellt sich dann die Frage, ob man dieses Problem über anderen Ringen entscheiden kann.

Eine übliche Verallgemeinerung der Entscheidung der Lösbarkeit diophantischer Mengen auf einen Integritätsring R (wir sagen *H10 über* R) ist die Betrachtung von Gleichungen mit Koeffizienten und Lösungen in R.
Man kann zeigen, dass für einen Integritätsring R, dessen Quotientenkörper nicht den algebraischen Abschluss des Primkörpers[1] enthält, folgende Aussagen äquivalent[2] sind:

- H10 ist über R lösbar,
- die existenzielle Theorie $\mathrm{Th}_{\exists}(R)$ von R ist entscheidbar.

Die existentielle Theorie der ganzen Zahlen beispielsweise ist die Menge aller wahren Aussagen der Form

$$\exists x_1, \ldots, \exists x_n \;\; F(x_1, \ldots, x_n)$$

für $x_1, \ldots, x_n \in \mathbb{Z}$, wobei $F(x_1, \ldots, x_n)$ eine quantorenfreie Konjunktion von Disjunktionen von Polynomgleichungen ist. Das zugehörige Entscheidungsproblem ist die Frage, ob eine vorliegende Formel dieser Art wahr oder falsch ist. Aus der negativen Lösung des 10. Hilbertproblems folgt also die Unentscheidbarkeit der existenziellen Theorie der ganzen Zahlen.

Wir wissen, dass H10 über $\mathbb{Z}$ unlösbar ist. Und vermutlich würde sich Hilbert mit dieser Antwort zufrieden geben. Dennoch stellt sich die Frage, ob Hilberts Interesse tatsächlich der Lösbarkeit diophantischer Gleichungen über den ganzen Zahlen galt. So vermutet Matijasevič, dass einzig Hilberts Optimismus die Formulierung von H10 auf ganze Zahlen beschränkte. Ein Algorithmus zur Lösung diophantischer Gleichungen über $\mathbb{Z}$ würde es uns auch erlauben, diese über $\mathbb{Q}$ zu lösen. Es liegt die Vermutung nahe, dass Hilbert mit einem Algorithmus über $\mathbb{Z}$ eben auch das Problem über den rationalen Zahlen lösen wollte. Insbesondere die Tatsache, dass bereits Diophantos[3] die Lösung algebraischer Gleichungen in rationalen Zahlen betrachtete, unterstützt diese Vermutung.

[1] Es ist bekannt, dass Primkörper von Körpern mit Charakteristik 0 isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen sind. Ist die Charakteristik eine Primzahl p, so ist der Primkörper isomorph zum Restklassenkörper $\mathbb{F}_p$ ([Bos09, Satz 2 in Kapitel 3.1]).
[2] Koe14, Observation 4.1.
[3] Diophantos von Alexandria war ein antiker griechischer Mathematiker und gilt als bedeutendster Algebraiker der Antike. Die diophantischen Gleichungen sind nach ihm benannt.

H10 ist unter anderem lösbar über $\mathbb{C}$[4] und $\mathbb{R}$[5]. Man kann H10 auch über algebraischen Zahlkörpern oder Funktionskörpern betrachten. Für manche dieser Körper ist die Unlösbarkeit gezeigt (vgl. [Koe14, Abschnitt 6]).
Hilberts 10. Problem über $\mathbb{Q}$ ist hingegen noch offen und damit die Frage nach der Entscheidbarkeit der existenziellen Theorie der rationalen Zahlen. Um die negative Lösung von H10 über $\mathbb{Z}$ auf die rationalen Zahlen zu übertragen, ist eine existentielle Definition von $\mathbb{Z}$ in $\mathbb{Q}$ notwendig. Dadurch könnte man $\mathrm{Th}_{\exists}(\mathbb{Z})$ in $\mathrm{Th}_{\exists}(\mathbb{Q})$ interpretieren und die negative Lösung übertragen. Die Frage, ob man $\mathbb{Z}$ existenziell in $\mathbb{Q}$ definieren kann, ist allerdings auch noch unbeantwortet. Ein anderer Ansatz für die Lösung von H10 über $\mathbb{Q}$ ist die Betrachtung von Ringen zwischen $\mathbb{Z}$ und $\mathbb{Q}$. Auf diese Weise versucht man, sich der Lösung über $\mathbb{Q}$ zu nähern.

Wir sehen also, dass Hilberts optimistische Forderung nach einem Algorithmus zur Entscheidung diophantischer Mengen weitaus mehr Fragen aufwirft, als man zunächst vermuten würde. Darüber hinaus liefert H10 interessante Verbindungen zur mathematischen Logik und zu offenen Fragen aus verschiedenen Bereichen der Mathematik.
Auf diese Weise schafft es David Hilbert mehr als 100 Jahre nach der Formulierung seiner Problemliste noch immer, dass Mathematiker auch heute interessiert den Fragen um die Entscheidung diophantischer Mengen nachgehen.

[4] $\mathbb{C}$ ist algebraisch abgeschlossen, also hat jede Gleichung vom Grad größer 0 eine Lösung.
[5] Das folgt aus Alfred Tarski's Untersuchungen von semialgebraischen Mengen.

Literaturverzeichnis

[Bos09] Siegfried Bosch. *Algebra*. 6. Auflage. Springer-Lehrbuch. Springer Berlin Heidelberg, 2009.

[Dav73] Martin Davis. „Hilbert's tenth problem is unsolvable“. In: *Amer. Math. Monthly* 80 (1973), S. 233–269.

[DMR76] Martin Davis, Yuri Matijasevič und Julia Robinson. „Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution“. In: *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*. Amer. Math. Soc., Providence, R. I., 1976, S. 323–378.

[Her75] I. N. Herstein. *Topics in algebra*. 2nd Edition. John Wiley, New York, 1975.

[Hil00] David Hilbert. „Mathematische Probleme“. In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* (1900). S. 253-297. The given talk is available at https://www.math.uni-bielefeld.de/~kersten/hilbert/rede.html.

[HMU01] John E. Hopcroft, Rajeev Motwani und Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. 2nd Edition. Addison-Wesley Publishing Co., Reading, Mass., 2001.

[Koe14] Jochen Koenigsmann. „Undecidability in number theory“. In: *Model theory in algebra, analysis and arithmetic*. Bd. 2111. Lecture Notes in Math. Springer, Heidelberg, 2014, S. 159–195.

[LP98] Harry Lewis und Christos H. Papadimitriou. *Elements of the Theory of Computation*. 2nd Edition. Prentice-Hall, 1998.

[Mat71] Ju. V. Matijasevič. „A Diophantine representation of the set of prime numbers“. In: *Dokl. Akad. Nauk SSSR* 196 (1971), S. 770–773.

[Mat96] Yuri Matijasevič. „Hilbert's tenth problem: what can we do with Diophantine equations?“ English version of a talk given by the author. Available at http://logic.pdmi.ras.ru/~yumat/personaljournal/H10history/H10histe.pdf. French version published in *La recherche de la vérité, Écrit. Math.,281–305, ACL-Éd. Kangourou, Paris, 1999*, 1996.

[MR75] Yuri Matijasevič und Julia Robinson. „Reduction of an arbitrary Diophantine equation to one in 13 unknowns“. In: *Acta Arith.* 27 (1975). Collection of articles in memory of Juriĭ Vladimirovič Linnik, S. 521–553.

[Poo08] Bjorn Poonen. „Undecidability in number theory“. In: *Notices Amer. Math. Soc.* 55.3 (2008), S. 344–350.

[Sch14] Ralf Schindler. *Set Theory*. Universitext. Exploring Independence and Truth. Springer, Cham, 2014.

[Sip06] Michael Sipser. *Introduction to the Theory of Computation*. 2nd Edition. Course Technology, 2006.

Plagiatserklärung

Hiermit versichere ich, dass die vorliegende Arbeit über

Hilberts 10. Problem: Diophantische Mengen sind nicht entscheidbar

selbstständig verfasst worden ist, dass keine anderen Quellen und Hilfsmittel als die angegebenen benutzt worden sind und dass die Stellen der Arbeit, die anderen Werken – auch elektronischen Medien – dem Wortlaut oder Sinn nach entnommenen wurden, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht worden sind.

Justin Dreyer, Wettringen, den 13. Juni 2016

Ich erkläre mich mit einem Abgleich der Arbeit mit anderen Texten zwecks Auffindung von Übereinstimmungen sowie mit einer zu diesem Zweck vorzunehmenden Speicherung der Arbeit in eine Datenbank einverstanden.

Justin Dreyer, Wettringen, den 13. Juni 2016