Handout: Listen in Peano Arithmetik

Nico Beck

January 3, 2025

In diesem Dokument geht es um das fünfte Kapitel aus Kayes Buch *Models of Peano Arithmetic*[1]. Das Kapitel ist sehr präzise und dadurch leider schwer verständlich. Was ich euch anbieten kann ist eine weniger präzise Zusammenfassung des Inhalts, die euch vielleicht hilft den richtigen Text besser zu verstehen. Am besten lest ihr als zuerst mein Handout als eine Art Einführung, und danach den Orginaltext von Kaye.

Ich werde zunächst die zugrunde liegende Zahlentheorie auf informelle Art erklären, und dann Stück so Stück so unformulieren, dass sie in der formellen Sprache der Peano Arithmetik ausgeführt werden kann. Die Zahlentheorie selber ist nicht so schwer, aber der Umstand, dass wir in PA keine Summen und Produkte bilden können, wird das Argument leider unverhältnismäßig kompliziert machen. Was wir im ganzen Text benötigen werden ist Teilen mit Rest.

Lemma 1. (*Teilen mit Rest*) PA zeigt den folgenden Satz. Gegeben zwei Zahlen x und y mit $y \neq 0$ gibt es genau zwei Zahlen s, r so dass $x = sy + r$ und $r < y$.

Der Beweis des Lemmas findet sich in jedem Zahlentheoriebuch, und kann eins zu eins in die formale Sprache übertragen werden. Deswegen überspringen ich den Beweis. Wichtig ist nur, dass wir die Sprache von PA konservativ um ein zweistelliges Funktionssymbol $\mathsf{remainder}$ erweitern können. Dafür verwenden wir ein folgende Theorem aus dem Buch *Introduction to Mathematical Logic* von Eliott Mendelson[2]. Ich habe das Theorem nur übertragen und übersetzt.

Theorem 1. (*Erweiterungen Sprachen erster Stufe.*) Nehme an wir haben eine Signatur S (bestehend aus Prädikats- und Funktionssymbolen) und die ihr zugehörige Sprache L. Nehme an T ist eine in der Sprache von L und Logik erster Stufe formulierte Theorie, und nehme zusätzlich an, dass $\varphi(\mathsf{x}, \mathsf{y}, \mathsf{z})$ eine Formel der Sprache L in drei freien Variablen ist, so dass $T \vdash \forall \mathsf{x} \forall \mathsf{y} \exists! \mathsf{z} \varphi(\mathsf{x}, \mathsf{y}, \mathsf{z})$. In anderen Worten, die Theorie T weiß, dass die Formel φ eine zweistellige Funktion beschreibt. Sei nun S' die Signatur, die wir bekommen, wenn wir zu S ein neues zweistelliges Funktionssymbol f hinzufügen, und sei L' die zu S' gehörende Sprache. Sei T' die Theorie, die entsteht, wenn wir zusätzlich zu den Sätzen von T noch das neue Axiom

$$\forall \mathsf{x} \forall \mathsf{y} \varphi(\mathsf{x}, \mathsf{y}, \mathsf{f}(\mathsf{x}, \mathsf{y}))$$

hinzufügen. Dann gibt es eine automatische Methode Formeln ϕ aus der Sprache L' in Formel $\phi^{\#}$ der Sprache L umzuwandeln, so dass die folgenden Bedingungen erfüllt sind.

(i) Wir haben $\phi^{\#} = \phi$ für jede Formel ϕ die das neue Symbol f nicht verwendet, also bereits eine Formel der Sprache L ist.

(ii) In der erweiterten Theorie T' sind ϕ und $\phi^{\#}$ äquivalent.

(iii) Eine Formel ϕ ist in der erweiterten Theorie T' genau dann beweisbar, wenn $\phi^{\#}$ von T bewiesen werden kann.

(iv) Der Prozess $\phi \mapsto \phi^{\#}$ kommutiert mit dem Bilden logischer Verküpfungen. Das bedeutet zum Beispiel, dass $(\phi \to \psi)^{\#} = \phi^{\#} \to \psi^{\#}$, aber auch $(\forall \mathsf{x} \phi)^{\#} = \forall \mathsf{x}\, \phi^{\#}$.

Der Beweis findet sich in Kapitel 2.9 von Mendelsons Buch. Im Endeffekt bedeutet das nur, dass wir in Beweisen das Funktionssymbol remainder frei verwenden dürfen und werden. Ausgestattet mit dem neuen Funktionssymbol können wir die Gödelsche β-Funktion auch innerhalb der formalen Sprache aufschreiben. Es ist

$$\beta(a, m, i) = \mathsf{remainder}(a, m(i+1)+1)$$

Außerdem werden wir das zweistellige Funktionssymbol $-$ und entsprechende Rechenregeln in Beweisen verwenden. Für uns ist $x - y = 0$ falls y größer als x ist. Die normalen Rechenregeln gelten so leider nur noch relativ zu der Situation angemessenen Ungleichungen. Gödels Lemma lautet nun wie folgt.

Lemma 2. (*Gödels Lemma*) Für jede Folge $x_0, ..., x_n$ von Zahlen gibt es eine Code a, m, so dass $\beta(a, m, i) = x_i$ für $i = 0, ..., n$.

Beweis Wir schauen uns zunächst einen informellen Beweis in der Metasprache an. Ich habe den Beweis aus einem anderen Logikbuch [3, page 116], aber es ist vermutlich einfach der Standardbeweis. Weder die genaue Formulierung von Gödels Lemma, die oben steht, noch der Beweis selber können in PA ausgeführt werden. Deswegen werden wir uns danach anschauen, wie wir alle problematischen Schritte PA-gerecht umformulieren können.

Der erste Schritt unseres informellen Beweises ist es eine Zahl m zu finden, die größer als alle Zahlen x_i ist und für die $m(0+1)+1, m(1+1)+1, ..., m(n+1)+1$ paarweise teilerfremd sind. Das ist immer möglich. Jedes groß genuge Vielfache von $n!$ funktioniert. Um das zu sehen, setze $m = a(n!)$ und nehme an eine Primzahl p teilt sowohl $m(i+1)+1$ als auch $m(j+1)+1$. Dann teilt p auch die Zahl $m(i-j)$. Aber $i - j$ ist ein Faktor von m, also teilt p auch die Zahl m ohne Rest. Dann folgt $0 = m(i+1)+1 = 1$ modulo p, was unmöglich ist. Daher gibt es eine solche Primzahl p nicht. Wenn zwei Zahlen keinen gemeinsamen Primteiler haben, dann haben sie überhaupt keinen gemeinsamen Teiler. Also wissen wir, dass $m(i+1)+1$ und $m(j+1)+1$ teilerfremd sind.

Nun gibt es nach dem Chinesischen Restsatz eine Zahl a, so dass $\beta(a, m, i) = x_i$ für alle $i \leq n$. Damit wir das später in PA nachahmen können, konstruieren wir ein solches a nun explizit. Wir setzen

$$M_i = \prod_{\substack{j \neq i \\ j \leq n}} (m(j+1)+1)$$

und wir bemerken, dass die Zahl M_i jeweils teilerfremd zu $m(i+1)+1$ ist, und dass sie durch all $m(j+1)+1$ mit $j \neq i$ und $j \leq n$ ohne Rest geteilt werden kann. Wegen Bezouts Theorem gibt es Zahlen a_i, so dass $a_i M_i = 1$ modulo $m(i+1)+1$ ist. Wir wissen außerdem, dass $a_i M_i = 0$ modulo $m(j+1)+1$ für alle $j \neq i$. Das ist sehr vielversprechend. Setzen wir nun

$$a = \sum_{i=0}^{n} x_i a_i M_i,$$

dann können wir problemlos ausrechnen, dass a die notwendigen Gleichungen erfüllt. □

Was sind die problematischen Schritte in dem Beweis von Gödels Lemma, den wir gerade aufgeschrieben haben? Zunächst einmal redet das Lemma von einer Liste $x_0, x_1, ..., x_n$ von Zahlen, und das können wir in PA ja gerade noch nicht tun. Deswegen werden wir stattdessen folgendes modifiziertes Lemma in PA beweisen.

Lemma 3. (*Gödels Lemma in PA.*) Die Theorie PA zeigt, für alle a, m, x und n gibt es a', m', so dass $\beta(a', m', i) = \beta(a, m, i)$ für $i < n$ und $\beta(a', m', n) = x$. Außerdem können wir die neuen Codezahlen a', m' beliebig groß wählen. In Symbolen:

$$PA \vdash \forall \mathsf{a} \forall \mathsf{m} \forall \mathsf{x} \forall \mathsf{n} \exists \mathsf{a}' \exists \mathsf{m}' (\forall \mathsf{i} < \mathsf{n} (\beta(\mathsf{a}, \mathsf{m}, \mathsf{i}) = \beta(\mathsf{a}', \mathsf{m}', \mathsf{i})) \wedge \beta(\mathsf{a}', \mathsf{m}', \mathsf{n}) = \mathsf{x})$$

Natürlich ist *die Theorie PA zeigt* halb gelogen, denn das Lemma ist ein Lemma der um das Funktionszeichen β erweiterten Sprache. Intuitiv bedeutet das Lemma, dass wir den Code einer Liste in PA zum Code einer längeren Liste erweitern können. Interpretiert in der Metatheorie folgt aus diesem schwächeren Lemma natürlich sofort auch, per Induktion über n, das volle Lemma von Gödel. Im Beweis werden wir sehen, dass wir fast die selben Zahlen a und m bilden, wie wir es im ersten informellen Beweis getan haben. Nur, da wir keine Rekursion zur Verfügung haben um Fakultäten, Produkte und Summen zu definieren, müssen wir die Zahlen M_i, a und m schrittweise während einer großen Induktion herstellen. Das macht den Bewies leider sehr kompliziert und verschachtelt. Wir beginnen nun mit dem Beweis. Am Ende sammeln wir die Sätze, die wir benutzt haben aber noch nicht beweisen haben.

Beweis Wir zeigen zunächst, dass wir eine Zahl m' finden können, so dass m' größer als x ist und größer als $\beta(a, m, i)$ ist für alle $i < n$. Außerdem sollen $m'(i+1)+1$ und $m'(j+1)+1$ teilerfremd sein für $i < j \leq n$. Natürlich wissen wir, dass die richtige Zahl ein Vielfaches der Fakultät von n ist, aber da Fakultäten uns nicht zur Verfügung steht, bauen wir sie stattdessen Stück für Stück auf, indem wir das Induktionsschema von PA benutzen. Wir müssen leider auch die Eigenschaft von m' mitschleppen, die es uns im ersten Beweis erlaubt hat zu zeigen, dass die $m'(i+1)+1$ paarweise teilerfremd sind. Wir beweisen per Induktion über k die folgende Aussage.

Seine a, m und x fixe Zahlen. Für alle k gibt es ein m', so dass

(i) $m' > x$ und $m' > \beta(a, m, i)$ für alle $i < k$.

(ii) Für $i < j \leq k$ sind $m'(i+1)+1$ und $m'(j+1)+1$ teilerfremd.

(iii) Jede Zahl $0 < j \leq k$ teilt m'.

Wir können das natürlich auch wieder in Symbolen ausdrücken.

$$\begin{aligned} PA \vdash \forall \mathsf{a} \forall \mathsf{m} \forall \mathsf{x} \forall \mathsf{k} \exists \mathsf{m}' (\mathsf{x} < \mathsf{m}' \wedge \forall \mathsf{i} < \mathsf{k} (\beta(\mathsf{a}, \mathsf{m}, \mathsf{i}) < \mathsf{m}') \\ \wedge \forall \mathsf{j} \leq \mathsf{k} \, \forall \mathsf{i} < \mathsf{j} \, \mathsf{coprime}(\mathsf{m}'(\mathsf{i}+1)+1, \mathsf{m}'(\mathsf{j}+1)+1) \\ \wedge \forall \mathsf{j} \leq \mathsf{k} \, (\neg \mathsf{j} = 0 \rightarrow \mathsf{divides}(\mathsf{j}, \mathsf{k}))) \end{aligned}$$

Das ist in Essenz der Inhalt von Lemma 5.5. aus Kayes Buch. Wie angekündigt machen wir eine Induktion über k. Für $k = 0$ ist fast nichts zu tun, denn dort sind die Bedingungen (ii) und (iii) automatisch erfüllt. Wir müssen einfach nur eine Zahl größer als x finden, und das geht natürlich. Nun der Induktionsschritt. Wir haben ein m', dass die Bedingungen (i)-(iii) für k erfüllt und suchen ein neues m''. Setze $m'' = am'(k+1)$, wobei a einfach irgendein Faktor ist, so dass $m'' > \beta(a, m, k)$ ist. Es ist nun klar, dass die Bedingungen (i) und (iii) erfüllt sind, und wir müssen nur zeigen, dass die Zahlen $m''(i+1)+1$ mit $i \leq k+1$ paarweise teilerfremd

sind. Das Argument funktioniert genau wie in unserem ersten Beweis. Wähle $i < j \leq k+1$ und sei p eine Primzahl, die sowohl $m''(i+1)+1$ als auch $m''(j+1)+1$ teilt. Dann teilt die Primzahl p auch $m''(j-i)$. Da p eine Primzahl ist, folgt, dass p die Zahl m'' oder die Zahl $j-i$ teilt. Es ist aber $j-i \leq k$, und somit teilt jede Zahl die $j-i$ teilt automatisch auch m'', da wir Bedingung (iii) für m'' schon bestätigt haben. Also teilt die Primzahl p in jedem Fall m'' und wir sehen, dass $0 = m''(j+1)+1 = 1$ modulo p. Das ist unmöglich. Also gibt es keine solche Primzahl, und wir folgern, dass $m''(i+1)+1$ und $m''(j+1)+1$ teilerfremd sind. Das zeigt, dass wir unsere Zahl m' finden können. Bemerke, dass wir im Prinzip nur Schritt für Schritt ein Vielfaches einer Fakultät gebildet haben.

Das Lemma gilt für alle k, also insbesondere auch für $k = n$. Wir setzen $k = n$ und wählen uns ein entsprechendes m'. Als nächstes möchten wir a' finden. Auch hier müssen wir wieder Schritt für Schritt vorgehen und das Induktionsschema von PA benutzen. Da wir unser m zu m' geändert haben, funktioniert unser altes a gar nicht mehr für den Beginn der Folge. Als erstes finden wir ein a'', so dass das Paar a'', m' zumindest die Folge $\beta(a,m,0), \beta(a,m,0), ..., \beta(a,m,n-1)$ wieder richtig kodiert. Per Induktion über k wollen wir zeigen, dass die folgende Aussage wahr ist.

Für alle $k \leq n$ gibt es ein a'', so dass $\beta(a,m,i) = \beta(a'',m',i)$ für alle $i < k$.

Leider brauchen wir zu Konstruktion der Zahl a'' im Induktionsschritt nicht nur die vorherige Zahl a'' aus der Induktionsvoraussetzung, sondern wir brauchen auch die Zahlen M_i. Die wichtigen Eigenschaften von M_i sind, dass es von allen $m'(j+1)+1$ geteilt wird für $j \neq i$, und dass M_i und $m'(i+1)+1$ teilerfremd sind. Erschaffen wir also am besten zuerst die M_is. Per beschränkter Induktion über k zeigen wir folgendes.

Für alle $k \leq n$ gilt: Für alle $i \leq n$ gibt es eine Zahl M, so dass M und $m'(i+1)+1$ teilerfremd sind, und $m'(j+1)+1$ die Zahl M teilt für alle $j \neq i$ und $j \leq k$.

Natürlich ist das nur wahr unter der Annahme, dass m' die oben beschriebenen Eigenschaften erfüllt, also insbesondere dass die Zahlen $m'(i+1)+1$ paarweise teilerfremd sind. Das ist in Essenz der Inhalt von Lemma 5.4. in Kayes Text. Der Beweis erfolgt, wie angekündigt, per Induktion über k. Während wir k erhöhen werden wir nach und nach die Zahlen M_i erschaffen. Für $k = 0$ ist fast nichts zu tun. Wir müssen nur für jedes $i \leq n$ eine Zahl M finden, die teilerfremd zu $m'(i+1)+1$ ist und durch $m'(0+1)+1$ geteilt werden kann, falls $i \neq 0$ ist. Das ist einfach. Für $i = 0$ setzen wir $M = 1$ und für $i \neq 0$ setzen wir $M = m(0+1)+1$. Nun zum Induktionsschritt. Für $k > n$ ist die Formel trivialerweise wahr. Für den Induktionsschritt nehme wir also an, die Formel sei wahr für ein $k < n$. Sei nun $i \leq n$ beliebig. Per Annahme haben wir eine Zahl M, so dass M und $m'(i+1)+1$ teilerfremd sind, und $m'(j+1)+1$ die Zahl M teilt wenn $j \neq i$ und $j \leq k$. Falls $k+1 = i$ ist, lasse die Zahl M so wie sie ist. Sie erfüllt alle notwendigen Bedingungen. Falls nicht, setze $M' = M(m'(k+1+1)+1)$. Es ist klar, dass M' und $m'(i+1)+1$ immer noch teilerfremd sind, denn $m'(i+1)+1$ und $m'(k+1+1)+1$ sind ja teilerfremd per Konstruktion von m'. Auch ist es klar, dass M' die andere Bedingung erfüllt, also sind wir fertig.

Mit unserem Lemma in der Hand können wir uns nun an die richtige Aussage wagen. Per Induktion über k wollen wir zeigen, dass folgende Aussage wahr ist.

Für alle $k \leq n$ gibt es ein a'', so dass $\beta(a,m,i) = \beta(a'',m',i)$ für alle $i < k$.

Ist $k = 0$, so ist nichts zu tun. Nehme an, wir haben die Aussage für ein $k < n$ bereits gezeigt. Es sei a'' eine Zahl, die die Bedingung der Induktionshypothese erfüllt. Wir möchten nun ein a''' finden, dass die Bedingung für alle $i < k+1$ erfüllt. Unser Lemma gibt uns eine Zahl M, so dass M und $m'(k+1)+1$ teilerfremd sind, und außerdem jedes andere $m'(i+1)+1$ ein Teiler

von M ist. Bezouts Theorem gibt uns eine Zahl u, so dass $uM = 1$ modulo $m'(k+1)+1$. Wir setzen nun

$$a''' = a'' + a''m'(k+1)uM + \beta(a,m,k)uM$$

und können damit die folgenden Rechnungen machen. Modulo $m'(k+1)+1$ haben wir:

$$\begin{aligned} a''' &= a'' + a''m'(k+1)uM + \beta(a,m,k)uM \\ &= a'' + a''m'(k+1) + \beta(a,m,k) \\ &= a''(m'(k+1)+1) + \beta(a,m,k) \\ &= \beta(a,m,k) \end{aligned}$$

Das ist genau was wir wollten. In der nächsten Rechnung verwenden wir, dass $uM = 0$ ist modulo $m'(i+1)+1$, und außerdem verwenden wir die Induktionshypothese. Modulo $m'(i+1)+1$ mit $i < k$ können wir wie folgt rechnen.

$$\begin{aligned} a''' &= a'' + a''m'(k+1)uM + \beta(a,m,k)uM \\ &= a'' + 0 \\ &= \beta(a,m,i) \end{aligned}$$

Damit haben wir den Induktionsschritt geschafft. In Konsequenz kriegen wir unseren Code a'', m' für das Anfangssegment der Folge. Zum Schluss müssen wir nur noch ein a' finden, dass sowohl das Anfangssegment als auch die neue Zahl x, die wir hinzufügen wollten, korrekt kodiert. Das funktioniert genau wie der Induktionsschritt den wir gerade ausgeführt haben. Unser Lemma gibt uns ein M so dass M und $m'(n+1)+1$ teilerfremd sind, und außerdem jedes andere $m'(i+1)+1$ ein Teiler von M ist. Wir kriegen von Bezouts Theorem außerdem ein u für das $uM = 1$ modulo $m'(n+1)+1$. Wir setzen nun

$$a' = a'' + a''m'(n+1)uM + \beta(a,m,n)uM$$

und die gleichen Rechnungen wie zuvor zeigen nun, dass a' alle notwendigen Bedingungen erfüllt. □

Ich hoffe der Beweis ist elementar genug, dass ihr daran glaubt, dass er so wie er ist in PA ausgeführt werden kann. Ich möchte zum Schluss noch die unbewiesenen Aussagen sammeln, die wir verwendet haben.

- Wir haben mehrfach Bezouts Theorem verwendet. Bezouts Theorem besagt, dass wann immer x und y teilerfremd sind es eine Zahl $u < y$ gibt, so dass $uy = 1$ modulo x.
- Insbesondere gibt es mehrere ein-, zwei- und dreistellige zahlentheoretische Prädikate, die wir definieren müssten, und deren Eigenschaften wir benutzt haben. Dazu gehören: x ist eine Primzahl, x teilt y, x und y sind teilerfremd, $y = x$ modulo z. Besonders oft haben wir Rechenregeln für Rechnungen modulo einer festen Zahl z benutzt. Wir haben auch benutzt, dass zwei Zahlen genau dann teilerfremd sind, wenn sie keinen gemeinsamen Primfaktor haben.
- Der Beweis von Bezouts Theorem in Kayes Buch benutzt außerdem das Least Number Principle. PA zeigt folgenden Satz für jede Formel $\varphi(\mathsf{x})$ in der freien Variable x.

$$PA \vdash \exists \mathsf{x}\varphi(\mathsf{x}) \to \exists \mathsf{w_0}(\varphi(\mathsf{w_0}) \wedge \forall \mathsf{y}(\varphi(\mathsf{y}) \to \mathsf{w_0} \leq \mathsf{y}))$$

Um all die Details zu sehen schaut ihr am besten in das Buch von Kaye. Auf der anderen Seite, wenn ihr bereit seit soweit in die formale Sprache einzutauchen, dann ist vielleicht sogar sinnvoll ihr lernt eine:n Beweisassistent:in zu benutzen. Der Computer kann was Menschen nicht so gut können, nämlich mit Syntax umgehen, und er wird euch viel Arbeit abnehmen und Sicherheit geben, dass das was ihr tut richtig ist.

References

[1] Sadie Kaye. *Models of Peano arithmetic.* Oxford Logic Guides, 1991.

[2] Elliott Mendelson. *Introduction to mathematical logic.* Chapman and Hall/CRC, 2009.

[3] Peter Smith. *An introduction to Gödel's theorems.* Cambridge University Press, 2013.