

Die unzerlegbaren Lösungen der linearen Kongruenz

Klaus Pommerening
Fachbereich Mathematik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-6500 Mainz

Oktober 1986, redaktionelle Überarbeitung: 30. Januar 2010

Zu den Gegenständen der additiven Zahlentheorie gehören die linearen diophantischen Probleme. Schwierigkeiten treten insbesondere dann auf, wenn man Lösungen in natürlichen Zahlen sucht; \mathbb{N} steht übrigens in dieser Arbeit stets für $\{0, 1, 2, \dots\}$, \mathbb{N}_k für $\{k, k+1, \dots\}$. Hier eine kleine Auswahl typischer Aufgaben, wobei ich mich der Einfachheit halber stets auf nur eine Gleichung beschränke:

(1) **Die homogene Gleichung:** Gegeben ist $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, gesucht $x = (x_1, \dots, x_n) \in \mathbb{N}^n$ mit

$$a_1x_1 + \dots + a_nx_n = 0.$$

(2) **Die inhomogene Gleichung;** hier nimmt man im allgemeinen Koeffizienten ≥ 0 an: Gegeben ist $a \in \mathbb{N}^n$ und $q \in \mathbb{N}_1$, gesucht $x \in \mathbb{N}^n$ mit

$$a_1x_1 + \dots + a_nx_n = q.$$

(3) **Die lineare Kongruenz:** Gegeben sind $m \in \mathbb{N}_2$ und $a \in \mathbb{Z}^n$, gesucht ist $x \in \mathbb{N}^n$ mit

$$a_1x_1 + \dots + a_nx_n \equiv 0 \pmod{m}.$$

Die eigentümliche Schwierigkeit dieser Probleme liegt darin, dass es fast nur elementare Methoden zu ihrer Behandlung gibt; daher kommt es, dass man auf eine konkrete Frage meistens nur eine ganz einfache oder überhaupt keine Antwort erhält. Gelegentlich liefert eine trickreiche Anwendung elementarer Methoden allerdings ein nichttriviales Ergebnis.

Über die inhomogene Gleichung (2) gibt es eine umfangreiche Literatur; als Einstieg geeignet sind die Abschnitte A10, D04 und P56-80 von [11], das dritte Kapitel von [1], [9], [3] und [4]. Typische Fragen sind: Für welche q gibt es Lösungen (das Briefmarken- oder Münzproblem), und wieviele sind es dann (Untersuchung der Anzahlfunktion)? Besonders bekannt ist natürlich

der Fall $a_1 = 1, \dots, a_n = n$, wo die Lösungen x genau den Partitionen von q in Stücke $\leq n$ entsprechen.

Über die beiden homogenen Probleme, die Gleichung und die Kongruenz, ist dagegen fast nichts bekannt. Einzelne Lösungen in großer Zahl anzugeben, ist trivial. Schwierig ist es, einen Überblick über alle Lösungen zu finden, und zu meiner Überraschung habe ich einige wesentliche Aussagen nirgends gefunden; das mag daran liegen, dass die einfachen Beispiele ein wirres Bild ergeben, hinter dem ordnende Prinzipien nicht ohne weiteres zu erkennen sind. Daher will ich in dieser Arbeit einige Ergebnisse über die lineare Kongruenz vorstellen und in einer folgenden die lineare Gleichung behandeln. Allerdings kann ich oft noch nicht die optimale Aussage beweisen und formuliere daher an den entsprechenden Stellen Probleme, deren weitere Behandlung aussichtsreich erscheint.

Sowohl die lineare Kongruenz als auch die lineare Gleichung haben eine direkte Deutung in der Invariantentheorie, und auf diesem Wege bin ich auf sie gestoßen. Diesen Zusammenhang erläutere ich im letzten Abschnitt dieser Arbeit.

Ich will zuerst die zentrale Aufgabe eingrenzen. Bei beiden Problemen (1) und (3) bildet die Lösungsmenge eine Unter-Halbgruppe $H \leq \mathbb{N}^n$ mit der Eigenschaft

$$x, y \in H, \quad x - y \in \mathbb{N}^n \implies x - y \in H,$$

also eine „volle“ Unter-Halbgruppe im Sinne von [6]. Die Halbgruppe \mathbb{N}^n trägt die (teilweise) Ordnung $x \leq y : \iff x - y \in \mathbb{N}^n$. Sei M die Menge der minimalen Elemente > 0 von H . Man sieht sofort:

- M erzeugt H , und jedes Erzeugendensystem von H enthält M .
- M besteht genau aus den unzerlegbaren Elementen von H , d. h., aus den $x \in H - \{0\}$ mit

$$x = y + z, \quad y, z \in H \implies y = 0 \text{ oder } z = 0.$$

- M ist vollständig ungeordnet, d. h., je zwei Elemente sind unvergleichbar.

Aus einem Lemma von Dickson, [2] oder [10, S. 52], folgt, dass M endlich ist; dieses Lemma beweist man übrigens ganz einfach durch Induktion über n . Jede volle Unter-Halbgruppe H von \mathbb{N}^n hat also ein kanonisches minimales Erzeugendensystem, das endlich ist und aus den unzerlegbaren Elementen von H besteht. *Achtung*: Nicht jede Unter-Halbgruppe von \mathbb{N}^n ist endlich erzeugt, zum Beispiel $H = \{(p, q) \mid p \geq 1\}$.

Damit stellt sich für die lineare Gleichung (1) und die lineare Kongruenz (3) jeweils die Aufgabe, die unzerlegbaren Lösungen zu bestimmen. Sie wird aufgegliedert in die sinnvollen Teilaufgaben:

(I) Finde möglichst starke Ungleichungen für die Koordinaten einer unzerlegbaren Lösung.

(II) Gib einen möglichst effizienten Algorithmus zum Auffinden aller unzerlegbaren Lösungen.

(III) Bestimme die Anzahl aller unzerlegbaren Lösungen, oder gib wenigstens gute Abschätzungen für diese Anzahl an.

Dabei wird sich erwartungsgemäß herausstellen, dass diese Anzahl von den Parametern, wie etwa der Zahl der Variablen oder der Koeffizientengröße, im wesentlichen exponentiell abhängt; insbesondere ist die Komplexität des Algorithmus in (II) auf jeden Fall exponentiell.

1 Reduktion auf einen Spezialfall

Sei $n \in \mathbb{N}_1$, $a_1, \dots, a_n \in \mathbb{Z}$. Gesucht sind die unzerlegbaren Lösungen $x \in \mathbb{N}^n$ der linearen Kongruenz

$$(A) \quad a_1x_1 + \dots + a_nx_n \equiv 0 \pmod{m}.$$

Für $r = 0, \dots, m-1$ sei

$$I_r := \{i = 1, \dots, n \mid a_i \equiv r \pmod{m}\},$$

also $\{1, \dots, n\} = I_0 \cup \dots \cup I_{m-1}$. Sei weiter L'_m die Menge der unzerlegbaren Lösungen $y = (y_0, \dots, y_{m-1}) \in \mathbb{N}^m$ der speziellen Kongruenz

$$(K'_m) \quad 0 \cdot y_0 + 1 \cdot y_1 + \dots + (m-1) \cdot y_{m-1} \equiv 0 \pmod{m}.$$

Zu jedem $y \in L'_m$ wählt man beliebige $x_1, \dots, x_n \in \mathbb{N}$ mit

$$\sum_{i \in I_r} x_i = y_r \quad \text{für } r = 0, \dots, m-1.$$

Klar, dass dann $x \in \mathbb{N}^n - 0$ minimal unter den Lösungen von (A) ist; ebenso klar, dass man jede minimale Lösung x auf diesem Weg erhält.

Man kann noch etwas weiter reduzieren. Jedes $y \in L'_m$ hat trivialerweise eine der Gestalten

- $y_0 = 1, y_1 = \dots = y_{m-1} = 0$,
- $y_0 = 0, (y_1, \dots, y_{m-1}) \in \mathbb{N}^{m-1}$ unzerlegbare Lösung der Kongruenz

$$(K_m) \quad 1 \cdot y_1 + \dots + (m-1) \cdot y_{m-1} \equiv 0 \pmod{m}.$$

Sei L_m die Menge der unzerlegbaren Lösungen von (K_m) . Dann ist gezeigt:

Satz 1 Man erhält alle unzerlegbaren Lösungen x von (A) auf eine der beiden folgenden Weisen:

- a) Für $i \in I_0$ setzt man $x_i = 1, x_j = 0$ für $j \neq i$.
 b) Zu jedem $y \in L_m$ wählt man $x_i \in \mathbb{N}$ für $i \in I_1 \cup \dots \cup I_{m-1}$ mit

$$\sum_{i \in I_r} x_i = y_r \quad \text{für } r = 1, \dots, m-1.$$

Bevor dieses Prinzip angewendet wird, zunächst ein Hilfssatz.

Hilfssatz 1 Sei $x \in \mathbb{N}^n$ eine unzerlegbare Lösung von (A). Dann ist

$$x_1 + \dots + x_n \leq m.$$

Beweis. Sei x eine Lösung von (A) mit $x_1 + \dots + x_n \geq m + 1$; zu zeigen: x ist zerlegbar.

Nun gibt es sicher $u \in \mathbb{N}^n$ mit $0 \leq u_i \leq x_i$ und $u_1 + \dots + u_n = m$. Seien $e_1 = (1, 0, \dots, 0), \dots, e_n$ die kanonischen Einheitsvektoren. Dann sind in der linear geordneten Menge der

$$0, e_1, \dots, u_1 e_1, u_1 e_1 + e_2, \dots, u_1 e_1 + u_2 e_2, \\ \dots, u_1 e_1 + \dots + u_n e_n = u$$

schon $m + 1$ verschiedene Elemente von \mathbb{N}^n . Also gibt es zwei davon, deren Koeffizientensummen modulo m kongruent sind. Ihre Differenz ergibt eine Lösung v von (A) mit $0 < v < x$. \diamond

Bemerkung. Genauso zeigt man: Sei $\Omega \subseteq \mathbb{Z}^n$ ein Gitter vom Index $\leq m$. Sei $Q = [0, r] \subseteq \mathbb{R}^n$ ein abgeschlossener Quader mit $r_1, \dots, r_n \in \mathbb{N}$, $r_1 + \dots + r_n = m$. Dann enthält Q einen Gitterpunkt $\neq 0$ von Ω . Um die Schlussweise von Hilfssatz 1 anzuwenden, beachtet man, dass Ω der Kern des Homomorphismus

$$\alpha: \mathbb{Z}^n \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad x \mapsto a_1 x_1 + \dots + a_n x_n \pmod{m}.$$

ist.

Nun zur Anwendung von Satz 1.

Korollar 1 Sei $N(a)$ die Anzahl der unzerlegbaren Lösungen von (A). Dann gilt

$$N(a) \leq \binom{n+m-1}{m},$$

und bei geeigneter Wahl von a wird diese Schranke angenommen. Genauer gilt

$$N(a) = n_0 + \sum_{y \in L_m} \left(\prod_{r=1}^{m-1} \binom{n_r + y_r - 1}{y_r} \right)$$

mit $n_r = \#I_r$.

Beweis. Die erste Aussage folgt direkt aus dem Hilfssatz: Zu gegebenen x_1, \dots, x_{n-1} gibt es höchstens ein x_n , so dass $(x_1, \dots, x_{n-1}, x_n)$ unzerlegbare Lösung von (A) ist, und dann ist notwendig $x_1 + \dots + x_{n-1} \leq m$. Die Anzahl der unzerlegbaren Lösungen ist also höchstens gleich der Anzahl der Möglichkeiten, x_1, \dots, x_{n-1} mit $x_1 + \dots + x_{n-1} \leq m$ zu wählen, also $\binom{n+m-1}{m}$. Die genaue Formel für $N(a)$ folgt aus Satz 1: Es gibt $\binom{n_r+y_r-1}{y_r}$ Möglichkeiten, y_r in x_i mit $\sum_{i \in I_r} x_i = y_r$ aufzuspalten. Die Schranke $\binom{n+m-1}{m}$ wird von $N(a)$ angenommen, wenn $n_1 = n$: Der Summand für $y \in L_m$ gibt 0 außer im Fall $y = (m, 0, \dots, 0)$. \diamond

Die Reduktion auf den Spezialfall (K_m) klappt also gut für einen Algorithmus zur Konstruktion aller unzerlegbaren Lösungen und für Bereichsabschätzungen, also die Probleme (I) und (II) aus der Einleitung. Für Anzahl-Abschätzungen ist der Nutzen, wie er im obigen Korollar zum Ausdruck kommt, zunächst nur gering, da dort die Kenntnis aller unzerlegbaren Lösungen von (K_m) vorausgesetzt wird.

Problem. Finde für den allgemeinen Fall (A) Methoden zur Abschätzung der Zahl der unzerlegbaren Lösungen, die von (K_m) höchstens analoge Abschätzungen, nicht aber die explizite Kenntnis der Lösungen voraussetzen. Da das wahrscheinlich zu viel verlangt ist, sind auch Ergebnisse für spezielle Klassen von Koeffizienten-Tupeln $a \in \mathbb{N}^n$ erstrebenswert.

2 Wo liegen die unzerlegbaren Lösungen?

Für jede unzerlegbare Lösung $x \in \mathbb{N}^{m-1}$ der Kongruenz

$$(K_m) \quad x_1 + \dots + (m-1)x_{m-1} \equiv 0 \pmod{m}$$

wissen wir aus Hilfssatz 1, dass $x_1 + \dots + x_{m-1} \leq m$. Es ist aber eine wesentlich stärkere Aussage möglich. Zunächst ein weiterer Hilfssatz.

Hilfssatz 2 Seien $r \in \mathbb{N}$ und $m \in \mathbb{N}_1$ mit $2r \leq m$. Seien $t_1, \dots, t_r \in \{1, \dots, m-1\}$ lauter verschiedene Zahlen. Für eine Teilmenge $I \subseteq \{1, \dots, r\}$ sei $S_I := \sum_{i \in I} t_i$. Außer für $I = \emptyset$ sei keine der Teilsummen S_I durch m teilbar. Dann repräsentieren die S_I mindestens $2r$ verschiedene Restklassen modulo m .

Beweis. Durch Induktion über r . Für $r = 0$ gibt es die eine Summe $S_\emptyset = 0$, und diese repräsentiert 1 Restklasse. Für $r = 1$ gibt es zwei Summen, 0 und t_1 , und sie repräsentieren 2 Restklassen.

Sei nun $r \geq 2$. Sei N die Zahl der verschiedenen Restklassen der 2^{r-1} Summen S_I mit $I \subseteq \{1, \dots, r-1\}$; nach Induktionsvoraussetzung ist $N \geq 2r-2$. Die Addition von t_r zu jedem S_I gibt die übrigen 2^{r-1} Summen, und auch diese ergeben genau N Restklassen, darunter die eine neue, $t_1 + \dots + t_r$,

die nur einmal vorkommt. Damit haben wir mindestens $N + 1$ Restklassen; wir hätten gerne $N + 2$.

Annahme: Die S_I mit $I \subseteq \{1, \dots, r\}$ repräsentieren nur $N + 1$ Restklassen. Dann bilden die S_I mit $I \subseteq \{1, \dots, r - 1\}$, $I \neq \emptyset$, genau $N - 1$ Restklassen a_1, \dots, a_{N-1} , und die S_I mit $r \in I$, $I \neq \{1, \dots, r\}$, repräsentieren genau die gleichen Restklassen a_1, \dots, a_{N-1} . Ist also $j \in \{1, \dots, N - 1\}$, so gilt $(a_j + t_r \bmod m) \in A := \{a_1, \dots, a_{N-1}\}$ oder $a_j + t_r \equiv t_1 + \dots + t_r \pmod{m}$. Die Gruppe $\mathbb{Z}/m\mathbb{Z}$ operiert auf sich selbst durch Addition von $t := t_r$. Dabei hat die Menge $A \subseteq \mathbb{Z}/m\mathbb{Z}$ genau einen Eingang $0 \mapsto t_r$ und genau einen Ausgang $t_1 + \dots + t_{r-1} \mapsto t_1 + \dots + t_r$. Die Bahn von 0 ist $\{0, t_r, \dots, (l - 1)t_r\}$ mit $l = m/\text{ggT}(t, m)$; sie verläuft etwa im Abschnitt $t_r, \dots, (p - 1)t_r$ in A , wobei $p \leq l - 1$ und notwendig $pt_r \equiv t_1 + \dots + t_r$. Außerdem kann es einige, etwa q , Bahnen geben, die ganz in A verlaufen und die Gestalt $\{a_j, a_j + t, \dots, a_j + (l - 1)t\}$ haben. Insbesondere gilt

$$N = ql + p,$$

$$t_1 + \dots + t_r \equiv pt \equiv qlt + pt = Nt \pmod{m}.$$

Da die Nummerierung der t_i keine Rolle gespielt hat, ist unter der obigen Annahme gezeigt:

$$t_1 + \dots + t_r \equiv Nt_i \pmod{m} \quad \text{für jedes } i = 1, \dots, r.$$

Sind $i, j \in \{1, \dots, r\}$ verschieden, so folgt $N \cdot (t_i - t_j) = k_{ij}m$ mit $k_{ij} \in \mathbb{Z}$; für $d := \text{ggT}(N, m)$ gilt also

$$\frac{N}{d}(t_i - t_j) \equiv 0 \pmod{\frac{m}{d}}, \quad t_i \equiv t_j \pmod{\frac{m}{d}}.$$

Eine Restklasse modulo m/d kann nur d verschiedene Zahlen $\in \{1, \dots, m - 1\}$ enthalten. Falls $r > d$, müssen also zwei der t_i gleich sein, Widerspruch.

Wir haben also mindestens $2r$ Restklassen, außer im Fall $N = 2r - 2$ und $d \geq r$. Dann ist notwendig $d = 2r - 2 = N$, also insbesondere $N|m$. Sei $m = eN$. Da $t_i \equiv t_j \pmod{e}$ für alle i und j , gibt es ein $a \in \{0, \dots, e - 1\}$ und r verschiedene Zahlen $s_1, \dots, s_r \in \{0, \dots, N - 1\}$ mit $t_i = a + es_i$ für $i = 1, \dots, r$. Wäre $a = 0$, so alle $t_i \equiv 0 \pmod{e}$, $t_1 + \dots + t_r \equiv Nt_i \equiv 0 \pmod{m}$, Widerspruch. Also ist $a \neq 0$. Dann ist aber $a \not\equiv 2a \pmod{e}$, d. h., modulo m sind alle Summen zweier t_i zu keinem einzelnen t_k kongruent. Damit haben wir die folgenden verschiedenen Restklassen-Repräsentanten:

- die leere Summe 0,
- die t_1, \dots, t_r selbst,
- die $r - 1$ Summen $t_1 + t_2, \dots, t_1 + t_r$,

also mindestens $2r$ Stück. \diamond

Für einen Vektor $x \in \mathbb{N}^n$ sei der Träger

$$\text{Supp}(x) := \{i = 1, \dots, n \mid x_i \neq 0\},$$

und seine Mächtigkeit

$$\sigma(x) := \#\text{Supp}(x).$$

Ferner sei die Koeffizientensumme mit

$$\lambda(x) := x_1 + \dots + x_n$$

bezeichnet. Für eine unzerlegbare Lösung $x \in \mathbb{N}^{m-1}$ von (K_m) ist die Koeffizientensumme umso stärker beschränkt, je größer der Träger ist:

Satz 2 Sei x eine unzerlegbare Lösung der Kongruenz (K_m) und $s \in \mathbb{N}$. Der Träger von x habe die Größe $\sigma(x) \geq s$. Dann gilt:

- (i) $\lambda(x) \leq m - s + 1$.
- (ii) $\lambda(x) = m - s + 1$ höchstens, wenn $\sigma(x) = s$.
- (iii) $2s \leq m + 1$; es gilt sogar $2s \leq m$, außer im Fall $m = 3$ und $x = (1, 1)$.
- (iv) Ist $\lambda(x) = m - s + 1$, so höchstens eine Koordinate $x_j \geq 2$.

Beweis. (i) und (ii) werden zusammen durch Induktion über s bewiesen. Für $s = 0$ ist $\lambda(x) < m + 1 = m - s + 1$. Sei nun $s \geq 1$.

(i) Da $\sigma(x) \geq s - 1$, ist $\lambda(x) \leq m - s + 2$ nach (i) für $s - 1$. Wäre $\lambda(x) = m - s + 2$, so $\sigma(x) = s - 1$ nach (ii) für $s - 1$. Also folgt $\lambda(x) \leq m - s + 1$.

(ii) Angenommen, $\lambda(x) = m - s + 1$ und $\sigma(x) \geq s + 1$. Dann ist jedenfalls $s + 1 \leq \lambda(x)$, also $2s \leq m$. Sei etwa $\{i_0, \dots, i_s\} \subseteq \text{Supp}(x)$ und $y := e_{i_0} + \dots + e_{i_s}$. Sei $\alpha(u) := u_1 + \dots + u_{m-1}$ für $u \in \mathbb{N}^{m-1}$. Für jede aufsteigende Kette

$$0 < u^{(1)} < \dots < u^{(s)} < u^{(s+1)} = y < \dots < u^{(m-s+1)} = x$$

mit $\lambda(u^{(\nu)}) = \nu$ sind die $\alpha(u^{(\nu)})$ paarweise inkongruent modulo m , sonst ergäbe eine Differenz $u^{(\mu)} - u^{(\nu)}$ eine Lösung $< x$. Wird das Stück zwischen y und x festgehalten, so bilden die $\alpha(u^{(\nu)})$ mit $s + 2 \leq \nu \leq m - s + 1$ genau $m - 2s$ verschiedene Restklassen. Also gibt es für $\alpha(u)$ mit $0 \leq u \leq y$ genau $2s$ verschiedene Möglichkeiten modulo m . Nach Hilfssatz 2 werden diese $2s$ Möglichkeiten aber schon von den $\sigma(u)$ mit $0 \leq u \leq y - e_{i_0}$ ausgeschöpft. Da bleibt nur der Ausweg $x = y$. Dann ist aber $s + 1 = \lambda(x) = m - s + 1$, also $2s = m \geq 2$ und $\sigma(x) = 1 + \frac{m}{2}$. Falls $m \geq 4$, gibt es unter den Paaren $(i, m - i)$ mit $1 \leq i < \frac{m}{2}$ mindestens eines mit $i, m - i \in \text{Supp}(x)$. Da x unzerlegbar ist, folgt $\text{Supp}(x) = \{i, m - i\}$, $s = 1$, Widerspruch. Falls $m = 2$, ist $x = s \in \mathbb{N}$, $\sigma(x) = 1 = s$, auch Widerspruch.

(iii) $s \leq \sigma(x) \leq \lambda(x) \leq m - s + 1$, also $2s \leq m + 1$. Ist $2s = m + 1$, so ist m ungerade, und es gibt $s - 1$ Paare $(i, m - i)$ mit $1 \leq i \leq \frac{m-1}{2} = s - 1$. Da $s = \sigma(x) = \lambda(x) = m - s + 1$, gilt $i, m - i \in \text{Supp}(x)$ für ein solches i , also $\text{Supp}(x) = \{i, m - i\}$, $s = 2$, $m = 3$, $x = (1, 1)$.

(iv) Für $m = 2$ ist das trivial; für $m = 3$ folgt es direkt aus der expliziten Angabe aller unzerlegbaren Lösungen: $(3, 0), (1, 1), (0, 3)$. Sei also o. B. d. A. $m \geq 4$. Dann ist $2s \leq m$ nach (iii) und $\sigma(x) = s$ nach (ii). Sei

$$y = \sum_{i \in \text{Supp}(x)} e_i.$$

Falls $x = y$, sind wir fertig. Andernfalls gibt es nach Hilfssatz 2 unter den $\alpha(u)$ mit $0 \leq u \leq y$ mindestens $2s$ verschiedene Restklassen modulo m . In jeder Kette

$$0 < u^{(1)} < \dots < u^{(s)} = y < u^{(s+1)} < \dots < u^{(m-s+1)} = x$$

bleiben für das Stück zwischen y und x (jeweils ausschließlich) gerade $m - 2s$ Möglichkeiten, so viele wie Plätze. Wird die Kette also an einer Stelle oberhalb y geändert, so müssen die α -Werte des alten und des neuen Elements übereinstimmen.

Angenommen, $x_i \geq 2$ und $x_j \geq 2$ mit $i \neq j$. Dann ist $y + e_i + e_j \leq x$, und zwischen y und $y + e_i + e_j$ gibt es genau die beiden Möglichkeiten $y + e_i$ und $y + e_j$. Es folgt $\alpha(y + e_i) \equiv \alpha(y + e_j)$, also $i = \alpha(e_i) \equiv \alpha(e_j) = j$, also $i = j$. \diamond

Die Übertragung dieses Satzes auf die allgemeinere Kongruenz (A) zwingt zu einer etwas schwerfälligen Formulierung und lohnt sich daher kaum. Den einfachen Spezialfall mit $s = 1$ kann man auch in [15] finden.

Aus Satz 1 und Satz 2 zusammen ergibt sich ein Suchalgorithmus für die Aufstellung des vollständigen Systems der unzerlegbaren Lösungen der Kongruenz (A), der für kleine Werte von m durchaus zufriedenstellend arbeitet. Da er aber nicht besonders originell ist, ist es wenig sinnvoll, ihn hier auszuformulieren.

3 Wieviele unzerlegbare Lösungen gibt es?

Sei $l(m)$ die Anzahl der unzerlegbaren Lösungen $x \in \mathbb{N}^{m-1}$ der linearen Kongruenz

$$(K_m) \quad x_1 + \dots + (m-1)x_{m-1} \equiv 0 \pmod{m}.$$

Aus dem Korollar zu Satz 1 folgt $l(m) \leq \binom{2m-2}{m}$. Aus Satz 2 erhält man sogar $x_1 + \dots + x_{m-1} \leq m - 1$ außer für die Lösungen $x = me_j$. Da man

statt dieser die Einheitsvektoren e_j mitzählt, erhält man die etwas schärfere Abschätzung $l(m) \leq \binom{2m-3}{m-1}$.

Mit Standard-Methoden kann man leicht eine obere Schranke für das Wachstum von $l(m)$ herleiten: Aus der Eulerschen Summenformel erhält man, vgl. [8, 1.2.11.2, S.110f.],

$$\ln(n!) = n \cdot \ln(n) - n + \frac{1}{2} \ln(n) + r_3,$$

wobei der Fehler r_3 durch Integration über das dritte Bernoulli-Polynom bestimmt wird; für unsere Zwecke reicht die Abschätzung $\frac{29}{32} \leq r_3 \leq \frac{121}{128}$. Daraus folgt eine Variante der Stirling-Formel:

Hilfssatz 3

$$e^{\frac{29}{32}} \cdot \left(\frac{n}{e}\right)^n \cdot \sqrt{n} \leq n! \leq e^{\frac{121}{128}} \cdot \left(\frac{n}{e}\right)^n \cdot \sqrt{n} \quad \text{für } n \geq 4.$$

Die Koeffizienten $e^{\frac{29}{32}} = 2.475\dots$ und $e^{\frac{121}{128}} = 2.573\dots$ liegen schon recht nah am asymptotischen Wert $\sqrt{2\pi} = 2.506\dots$. Die explizite Rechnung zeigt, dass die linke Ungleichung sogar für $n \geq 1$ gilt.

Korollar 1

$$\frac{\sqrt{2}}{e^{\frac{63}{64}}} \cdot \frac{4^n}{\sqrt{n}} \leq \binom{2n}{n} \leq \frac{\sqrt{2}}{e^{\frac{111}{128}}} \cdot \frac{4^n}{\sqrt{n}}$$

für $n \geq 2$, die rechte Ungleichung sogar für $n \geq 1$.

Beweis. Direkt aus dem Lemma, für $n < 4$ durch explizite numerische Rechnung. \diamond

Hier haben wir die Koeffizienten $\frac{\sqrt{2}}{e^{\frac{63}{64}}} = 0.528\dots$ und $\frac{\sqrt{2}}{e^{\frac{111}{128}}} = 0.594\dots$; ihr asymptotischer Wert ist $\frac{1}{\sqrt{\pi}} = 0.564\dots$. Da $\binom{2m-3}{m-1} = \frac{(2m-3)\cdots(m-1)}{1\cdots(m-1)} = \frac{1}{2} \binom{2m-2}{m-1}$, ist gezeigt:

Satz 3 Für die Anzahl $l(m)$ der unzerlegbaren Lösungen von (K_m) gilt

$$l(m) \leq \frac{1}{\sqrt{2} \cdot e^{\frac{111}{128}}} \cdot \frac{1}{\sqrt{m-1}} \cdot 4^{m-1} \leq \frac{1}{3 \cdot \sqrt{m-1}} \cdot e^{(m-1) \cdot \ln(4)}.$$

Das ist höchstens ein einfaches exponentielles Wachstum. Dabei ist Satz 2 aber bisher fast gar nicht ausgenutzt worden. Er liefert natürlich eine etwas bessere Abschätzung, ohne allerdings die Asymptotik zu verbessern.

Sei dazu o. B. d. A. $m \geq 4$. Dann hat der Träger einer unzerlegbaren Lösung höchstens $\lfloor \frac{m}{2} \rfloor$ Elemente. Für jedes $s \in \{1, \dots, \lfloor \frac{m}{2} \rfloor\}$ gibt es genau $\binom{m-1}{s}$ Möglichkeiten, eine s -elementige Teilmenge $S = \{i_1, \dots, i_s\} \subseteq \{1, \dots, m-1\}$ als Träger zu wählen. Jeder solche Träger trägt höchstens

s unzerlegbare Lösungen mit $\lambda(x) = m - s + 1$, alle übrigen erfüllen $\lambda(x) \leq m - s$; wählt man $x_{i_1}, \dots, x_{i_{s-1}}$ beliebig, so gibt es höchstens ein x_{i_s} , das sie zu einer Lösung ergänzt. Alle unzerlegbaren Lösungen auf S mit $\lambda(x) \leq m - s$ werden also eingefangen, wenn man Zahlen $y_1, \dots, y_{s-1} \geq 0$ mit $y_1 + \dots + y_{s-1} \leq m - 2s$ beliebig wählt, dazu $x_{i_\nu} = y_\nu + 1$ bildet und x_{i_s} passend wählt. Ihre Anzahl ist daher höchstens $\binom{m-2s+s-1}{s-1} = \binom{m-s-1}{s-1}$. Unter den so gezählten Vektoren sind genug Nicht-Lösungen, um die unzerlegbaren Lösungen mit $\lambda(x) = m - s + 1$ aufzufangen, d. h., die Gesamtzahl aller unzerlegbaren Lösungen mit Träger S ist $\binom{m-s-1}{s-1}$:

Ist $\lambda(x) = m - s + 1$, so $x_i = 1$ für alle $i \in S$ bis auf eines, etwa $x_{i_\nu} = m - 2s + 2$. Falls $\nu = s$, gibt es zu $y_1 = \dots = y_{s-1} = 0$, also $x_{i_1} = \dots = x_{i_{s-1}} = 1$, keine Wahl von $x_{i_s} \in \{1, \dots, m - 2s + 1\}$, so dass $(x_{i_1}, \dots, x_{i_s})$ eine Lösung ist. Falls $\nu \leq s - 1$, lässt die Wahl $y_\nu = m - 2s$, $y_\mu = 0$ sonst, also $x_{i_\nu} = m - 2s + 1$, $x_{i_\mu} = 1$ sonst für $\mu = 1, \dots, s - 1$, im Bereich $x_{i_1} + \dots + x_{i_s} \leq m - s$ nur noch die Wahl $x_{i_s} = 1$, und das ergibt dann auch eine Nicht-Lösung.

Daraus ergibt sich als Zusammenfassung:

Satz 4 Für die Anzahl $l(m)$ der unzerlegbaren Lösungen von (K_m) , $m \geq 4$, gilt

$$l(m) \leq \sum_{s=1}^{\lfloor \frac{m}{2} \rfloor} \binom{m-1}{s} \cdot \binom{m-s-1}{s-1}.$$

Eine untere Schranke für $l(m)$ beruht auf einer Idee von STANLEY [7]: Jede Lösung $x \in \mathbb{N}^{m-1}$ von

$$(P_m) \quad x_1 + 2x_2 + \dots + (m-1)x_{m-1} = m$$

ist eine unzerlegbare Lösung von (K_m) ; diese entsprechen genau den Partitionen von m außer der trivialen $m = m \cdot 1$. Es sind also $p(m) - 1$ Stück, wobei p die Partitionsfunktion ist. Leicht findet man weitere unzerlegbare Lösungen:

a) Sei $j \in \{1, \dots, m-1\}$ kein Teiler von m und $l \geq 1$ minimal mit $m|jl$. Dann ist $x_j = l$, $x_i = 0$ sonst, eine unzerlegbare Lösung. Das sind $m - d(m) + 1$ Stück, wobei

$$d(m) := \#\{j \in \{1, \dots, m\} \mid j|m\}.$$

(Die Fälle mit $j|m$ sind schon unter den Partitionen enthalten.)

b) Ist (x_1, \dots, x_{m-1}) eine unzerlegbare Lösung von (K_m) , so auch (x_{m-1}, \dots, x_1) . Sie ist dann neu, wenn x nicht symmetrisch für diese Spiegelungs-Operation ist und mindestens zwei Koordinaten $\neq 0$ hat. Von den $p(m) - 1$ Spiegelbildern der Lösungen von (P_m) kennen wir also schon

1. die, die nur eine Koordinate $\neq 0$ haben, also $d(m) - 1$ Stück,

2. die symmetrischen mit mindestens zwei Einträgen $\neq 0$; das sind $\lfloor \frac{m-1}{2} \rfloor$ Stück. Denn ist $x_{m-j} = x_j \leq 1$, so $jx_j + (m-j)x_{m-j} = mx_j \equiv 0 \pmod{m}$, also $x_j = x_{m-j} = 1$ und $x_i = 0$ sonst.

Zählen wir zusammen, so kommen wir auf:

Satz 5 Für die Anzahl $l(m)$ der unzerlegbaren Lösungen von (K_m) gilt

$$l(m) \geq 2 \cdot p(m) - 2 \cdot d(m) + \lfloor \frac{m}{2} \rfloor.$$

Um eine glatte Formel zu erhalten, fragen wir, wann $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor$ ist.

Hilfssatz 4 Sei $m = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktor-Zerlegung von $m \in \mathbb{N}_1$ mit $2 \leq p_1 < \dots < p_r$ und $e_i > 0$. Dann gilt:

- (i) $d(m) = (e_1 + 1) \cdots (e_r + 1)$.
- (ii) $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor \Leftrightarrow 4 \cdot (e_1 + 1) \cdots (e_r + 1) \leq m$.
- (iii) $(e_1 + 1) \cdots (e_r + 1) \leq m$.
- (iv) Ist ein $p_i^{e_i} \geq 4(e_i + 1)$ oder sind zwei davon jeweils $\geq 2(e_i + 1)$, so ist $4(e_1 + 1) \cdots (e_r + 1) \leq m$.
- (v) $4 \cdot d(m) \leq m$ außer für $m \leq 10$ und $m = 12, 14, 15, 16, 18, 20, 24, 30$.

Beweis. (i)-(iv) trivial.

(v) Dem Kriterium in (iv) entgehen nur die Teiler der Zahlen

$$2^4 \cdot 3 = 48, \quad 2^2 \cdot 3^2 = 36, \quad 2^2 \cdot 3 \cdot 5 = 60 \quad \text{und} \quad 2^2 \cdot 3 \cdot 7 = 84,$$

also außer den in (v) genannten Zahlen nur noch $m = 21, 28, 36, 42, 48, 60$ und 84 . Für diese kann man die Behauptung direkt verifizieren. \diamond

Korollar 1 $l(m) \geq 2 \cdot p(m)$ für $m \geq 7$.

Beweis. Außer für $m = 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24$ und 30 folgt das aus Satz 5 und Hilfssatz 4. Für diese übrigen 12 Werte von m müssen wir jeweils $2d(m) - \lfloor \frac{m}{2} \rfloor$ weitere unzerlegbare Lösungen von (K_m) finden, also der Reihe nach $1, 4, 2, 3, 6, 1, 1, 2, 3, 2, 4, 1$. Diese kann man leicht sogar unter denen mit zweielementigem Träger finden (vgl. auch Abschnitt 4). \diamond

Aus der bekannten Asymptotik der Partitionsfunktion [5] folgt:

Korollar 2 Sei $a \in \mathbb{R}$ mit $0 \leq a < \frac{1}{2\sqrt{3}}$ beliebig. Dann gilt

$$l(m) \geq \frac{a}{m} \cdot e^{\pi \sqrt{\frac{2m}{3}}} \quad \text{für fast alle } m \in \mathbb{N}_2.$$

Probleme. Die oberen Schranken aus Satz 3 und 4 sind noch erheblich zu grob. Ist $l(m) \leq a \cdot e^{b \cdot \sqrt{m}}$ für geeignete Konstanten a und b ? Gilt $l(m) \leq m \cdot p(m)$ für $m \geq 2$? Hier einige explizite Einzelwerte, die mit dem in Abschnitt 2 erwähnten Algorithmus leicht zu finden sind:

m	2	3	4	5	6	7	8	9	10	11
$l(m)$	1	3	6	14	19	47	64	118	169	327
$2 \cdot p(m)$	4	6	10	14	22	30	44	60	84	112
$m \cdot p(m)$	4	9	20	35	66	105	176	270	420	616

4 Die lineare Kongruenz mit zwei Unbekannten

Besonders gute Ergebnisse sind für den Fall $n = 2$ der linearen Kongruenz (3) zu erwarten; dieser Fall betrifft natürlich auch die Lösungen mit höchstens zweielementigem Träger im allgemeinen Fall. Die Ergebnisse sind im Prinzip bekannt, siehe [14], [15], [12], [13]. Ich kann hier allerdings eine besonders durchsichtige Herleitung anbieten. Betrachten wir also die Kongruenz

$$ax + by \equiv 0 \pmod{m}$$

mit o. B. d. A. $a, b \in \{1, \dots, m-1\}$. Sie lässt sich leicht auf den Fall $a = 1$ reduzieren:

Falls $\text{ggT}(a, b, m) =: d > 1$, sind die unzerlegbaren Lösungen genau diejenigen von $\frac{a}{d} \cdot x + \frac{b}{d} \cdot y \equiv 0 \pmod{\frac{m}{d}}$. Wir können also o. B. d. A. $\text{ggT}(a, b, m) = 1$ annehmen.

Falls $\text{ggT}(b, m) =: d > 1$, $\text{ggT}(a, b, m) = 1$, sind für $(x, y) \in \mathbb{N}_2$ die beiden folgenden Aussagen äquivalent:

- (i) (x, y) ist unzerlegbare Lösung von $ax + by \equiv 0 \pmod{m}$.
- (ii) $d|x$, und $(\frac{x}{d}, y)$ ist unzerlegbare Lösung von $a \cdot s + \frac{b}{d} \cdot t \equiv 0 \pmod{\frac{m}{d}}$.

Analog, wenn a und m nicht teilerfremd sind. Also können wir o. B. d. A. a mit m und b mit m als teilerfremd annehmen. Dann hat a modulo m ein Inverses c , $ac \equiv 1 \pmod{m}$, und die unzerlegbaren Lösungen sind dieselben wie die von $1 \cdot x + b' \cdot y \equiv 0 \pmod{m}$ mit $b' = bc \pmod{m}$. Daher wollen wir nun sehen, was über die unzerlegbaren Lösungen der Kongruenz

$$x + by \equiv 0 \pmod{m}$$

zu sagen ist, wobei $m \in \mathbb{N}_1$ und $b \in \mathbb{N}$ beliebig zugelassen sein sollen.

Auch hier findet man eine Reduktion auf kleineres m , die zu einer (zunächst) rekursiven (später iterativen) Bestimmung der unzerlegbaren Lösungen und ihrer Anzahl führt.

Hilfssatz 5 Seien $b, m \in \mathbb{N}_1$. Sei $(s, t) \in \mathbb{N}^2$ eine unzerlegbare Lösung von $s + bt \equiv 0 \pmod{m}$. Sei $u := \frac{s+bt}{m}$. Dann gilt:

- (i) $u = \lfloor \frac{bt}{m} \rfloor$, außer wenn $(s, t) = (m, 0)$.
- (ii) $t + u \leq m + b$; sogar $<$, außer wenn $(s, t) = (0, m)$.
- (iii) $(s, t + u)$ ist unzerlegbare Lösung von

$$(*) \quad x + by \equiv 0 \pmod{m + b}.$$

Beweis. (i) Ist $(s, t) \neq (m, 0)$, so $0 \leq s < m$, also $\frac{bt}{m} \leq u < \frac{u+bt}{m} = 1 + \frac{bt}{m}$.

(ii) Sei $(s, t) \neq (0, m)$, also $0 \leq t \leq m - 1$. Nach (i) ist $u < 1 + \frac{bt}{m}$ oder $t = 0, s = m, u = 1$. Im ersten Fall ist $t + u < m + \frac{bt}{m} \leq m + b \cdot \frac{m-1}{m} < m + b$. Im zweiten Fall ist $t + u = 1 < 2 \leq m + b$. Sei nun $(s, t) = (0, m)$; dann ist $u = b$ und $t + u = m + b$.

(iii) Falls $(s, t) = (m, 0)$, ist $(s, t + u) = (m, 1)$ unzerlegbare Lösung von $(*)$. Sei also jetzt $0 \leq s < m, 0 < t \leq m$. Zunächst ist $s + b \cdot (t + u) = u \cdot (m + b)$, also $(s, t + u)$ Lösung von $(*)$. Sei nun (x, y) eine Lösung von $(*)$ mit $0 < (x, y) \leq (s, t + u)$; dann ist $x + by = v \cdot (m + b)$ mit $1 \leq v \leq u$. Da $x \leq s < m \leq vm$, ist $by = vm + bv - x > bv$. Also ist $y > v$ und $x + b \cdot (y - v) = vm \equiv 0 \pmod{m}$. Wäre $y - v > t$, so $vm > b \cdot (y - v) > bt = um - s > (u - 1) \cdot m$, also $v \geq u, y > t + u$, Widerspruch. Also ist $y - v \leq t, 0 < (x, y - v) \leq (s, t), x = s, y = t + v, vm = um, v = u, (x, y) = (s, t + u)$. \diamond

Satz 6 Seien $b, m \in \mathbb{N}_1$. Die Zuordnung $(s, t) \mapsto (s, t + u)$ mit $u = \frac{s+bt}{m}$ ist eine Bijektion

- (a) von der Menge der unzerlegbaren Lösungen von $s + bt \equiv 0 \pmod{m}$
 (b) auf die Menge der unzerlegbaren Lösungen von $(*) \quad x + by \equiv 0 \pmod{m + b}$ außer $(m + b, 0)$.

Beweis. Die Abbildung existiert wegen Hilfssatz 5 und ist injektiv, weil jede unzerlegbare Lösung von $(*)$ durch ihre erste Koordinate bereits eindeutig festgelegt ist. Daß $(m + b, 0)$ nicht im Bild liegt, ist klar. Zu zeigen ist also noch die Surjektivität der Abbildung.

Sei also $(x, y) \in \mathbb{N}^2$ eine unzerlegbare Lösung $\neq (m + b, 0)$ von $(*)$, etwa $x + by = u \cdot (m + b)$ mit $u \in \mathbb{N}_1$. Aus Hilfssatz 5 (i) folgt

$$u = \lceil \frac{by}{m + b} \rceil < \frac{by}{m + b} + 1 < y + 1,$$

also $u \leq y$. Da $x + b \cdot (y - u) = um$, ist $(x, y - u)$ Lösung mod m . Ist sie unzerlegbar? Zunächst ist sie $\neq 0$, sonst wäre $x = 0, y = u, bu = um + ub$, Widerspruch. Sei $0 \leq (s, t) \leq (x, y - u)$ mit $s + bt \equiv 0 \pmod{m}$, etwa $s + bt = vm$ mit $0 \leq v \leq u$. Dann ist $s + b \cdot (t + v) = v \cdot (m + b)$ und $s \leq x, t + v \leq y - u + v \leq y$. Es folgt

$$s = x, \quad t + v = y, \quad v = u, \quad t = y - u$$

oder aber

$$s = 0, \quad t + v = 0, \quad t = 0.$$

Also hat (x, y) das Urbild $(x, y - u)$. \diamond

Für $b \in \mathbb{N}$ und $m \in \mathbb{N}_1$ sei nun $A(m, b)$ die Anzahl der unzerlegbaren Lösungen der Kongruenz $s + bt \equiv 0 \pmod{m}$.

Korollar 1 (i) $A(m, km) = 2$ für alle $m \in \mathbb{N}_1$ und $k \in \mathbb{N}$.

(ii) $A(m, 1) = m + 1$ für alle $m \in \mathbb{N}_1$.

(iii) A ist in der zweiten Variablen periodisch: $A(m, m + b) = A(m, b)$ für alle $m \in \mathbb{N}_1$ und $b \in \mathbb{N}$.

(iv) A ist in der ersten Variablen quasiperiodisch: $A(m + b, b) = 1 + A(m, b)$ für alle $m, b \in \mathbb{N}_1$.

(v) Ist $ab \equiv 1 \pmod{m}$, so ist $A(m, a) = A(m, b)$.

Beweis. (i) Die unzerlegbaren Lösungen sind $(m, 0)$ und $(0, 1)$.

(ii) Die unzerlegbaren Lösungen sind $(k, m - k)$ für $k = 0, \dots, m$.

(iii) $s + bt \equiv 0 \pmod{m} \Leftrightarrow s + (b + m)t \equiv 0 \pmod{m}$.

(iv) folgt direkt aus Satz 6.

(v) $s + at \equiv 0 \pmod{m} \Leftrightarrow bs + bat \equiv 0 \pmod{m} \Leftrightarrow t + bs \equiv 0 \pmod{m}$.

\diamond

Mit den Rekursionsformeln (iii) und (iv) läßt sich aus der Anfangsbedingung $A(m, 0) = 2$ die Tabelle aller $A(m, b)$ sehr effizient berechnen. Die Rekursion und auch ihr Beweis in [14], [15] scheinen mir wesentlich komplizierter zu sein.

Korollar 2 Seien $m, b \in \mathbb{N}_1$, und sei

$$r_0 = m, \quad r_1 = b, \quad \dots, \quad r_{i-1} = q_i r_i + r_{i+1}, \quad \dots, \quad r_{n-1} = q_n r_n$$

mit $0 < r_n < \dots < r_1$ die Euklidische Divisionskette, insbesondere $r_n = \text{ggT}(m, b)$. Ferner sei

$$\tilde{A}(m, b) = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} q_{2k+1}$$

die Summe der Quotienten mit ungerader Nummer. Dann gilt

$$A(m, b) = \begin{cases} \tilde{A}(m, b) + 1, & \text{falls } n \text{ ungerade,} \\ \tilde{A}(m, b) + 2, & \text{falls } n \text{ gerade.} \end{cases}$$

$A(m, b)$ berechnet sich also explizit aus dem Euklidischen Algorithmus oder, anders ausgedrückt, aus der Kettenbruch-Entwicklung von $\frac{m}{b}$.

Beweis. Sei $r_{n+1} := 0$. Aus Korollar 1 (iv) folgt sofort

$$A(m, b) = \begin{cases} q_1 + A(r_2, b), & \text{falls } n \geq 2, \\ q_1 - 1 + A(b, b), & \text{falls } n = 1, \end{cases}$$

und daraus sukzessive die Behauptung. \diamond

Korollar 3 *Unter den Voraussetzungen von Korollar 2 sind die ersten Koordinaten der unzerlegbaren Lösungen der Kongruenz $s + bt \equiv 0 \pmod{m}$ genau die Zahlen r_0 und*

$$r_{2i} - j \cdot r_{2i+1} \quad \text{für } 0 \leq i \leq \lfloor \frac{n-1}{2} \rfloor, \quad 1 \leq j \leq q_{2i+1},$$

und dazu noch die 0, falls n gerade.

Gewonnen werden sie, wenn man sie mit x_0, x_1, x_2, \dots bezeichnet, aus folgender Prozedur (in Pidgin-Pascal formuliert):

```

 $x_0 := m; i := 0;$ 
solange  $m > 0$ :
   $b := b \bmod m;$ 
  falls  $b = 0$ 
     $i := i + 1; x_i := 0; m = 0$ 
  sonst
    solange  $m \geq b$ :
       $m := m - b; i := i + 1; x_i := m$ 

```

5 Die Anzahl der unzerlegbaren Lösungen mit zweielementigem Träger

Für $m \in \mathbb{N}_1$ und $1 \leq k \leq m - 1$ sei $l_k(m)$ die Anzahl der unzerlegbaren Lösungen von (K_m) , deren Träger genau k Elemente hat. Der Einfachheit halber sei $m = p$ eine Primzahl ≤ 3 . Dann operiert die zyklische Gruppe $Z_{p-1} = (\mathbb{Z}/p\mathbb{Z})^\times$ auf der Menge der zweielementigen Teilmengen von $\{1, \dots, p-1\}$. Eine Bahn wird von den $\frac{p-1}{2}$ Mengen $\{r, p-r\}$ mit $1 \leq r \leq \frac{p-1}{2}$ gebildet. Ansonsten gibt es $\frac{p-3}{2}$ Bahnen, die aus je $p-1$ Mengen bestehen, darunter $\{1, j\}$ und $\{1, k\}$ mit $jk \equiv 1 \pmod{p}$. Die Anzahl der unzerlegbaren Lösungen mit gegebenem Träger ist auf jeder solchen Bahn konstant. Sei $a(p, j)$ die Anzahl aller unzerlegbaren Lösungen mit Träger $\{1, j\}$, $2 \leq j \leq p-1$; nach Korollar 2 zu Satz 6 ist $a(p, j) = \hat{A}(p, j)$ oder $\hat{A}(p, j) - 1$, je nachdem, ob die Euklidische Divisionskette für p und j gerade

oder ungerade Länge hat. (Achtung: In Abschnitt 4 wurden Lösungen mit Träger $\subseteq \{1, j\}$ gezählt, also auch die beiden mit einer Null-Komponente.) Insgesamt ist

$$l_2(p) = \frac{p-1}{2} \cdot a(p, p-1) + (p-1) \cdot \frac{1}{2} \cdot \sum_{j=2}^{p-2} a(p, j).$$

Satz 7 Für eine Primzahl $p \geq 3$ hat die lineare Kongruenz (K_p) genau

$$l_2(p) = \frac{p-1}{2} \cdot \sum_{j=2}^{p-1} a(p, j)$$

unzerlegbare Lösungen mit zweielementigem Träger.

Diese Formel ist zwar leicht auszuwerten, aber sie ist nicht so explizit, dass man mit ihr wunschlos glücklich sein kann. Außerdem wird sie, wenn man zu zusammengesetzten Moduln m übergeht, stark verunstaltet. Andererseits erlaubt sie auf einfache Weise, obere und untere Schranken anzugeben; diese beruhen auf der Abschätzung

$$\begin{aligned} \lfloor \frac{m}{j} \rfloor &\leq \tilde{A}(m, j) \leq \lfloor \frac{m}{j} \rfloor + (m \bmod j) - 1, \\ \lfloor \frac{m}{j} \rfloor - 1 &\leq a(m, j) \leq \lfloor \frac{m}{j} \rfloor + (m \bmod j) - 1. \end{aligned}$$

Für die untere Grenze folgt

$$\begin{aligned} \sum_{j=2}^{m-1} \lfloor \frac{m}{j} \rfloor &\geq \sum_{j=2}^{m-1} (\frac{m}{j} - 1) \geq -(m-2) + \int_{x=2}^m \frac{m}{x} dx \\ &= -(m-2) + m \cdot (\ln m - \ln 2) = m \cdot \ln m - m \cdot (1 + \ln 2) + 2. \end{aligned}$$

An der oberen Grenze gelten die Abschätzungen

$$\begin{aligned} \sum_{j=2}^{m-1} \lfloor \frac{m}{j} \rfloor &\leq \sum_{j=2}^{m-1} \frac{m}{j} \leq \int_{x=1}^{m-1} \frac{m}{x} dx = m \cdot \ln(m-1), \\ \sum_{j=2}^{m-1} (m \bmod j) &\leq \sum_{j=2}^{m-1} (j-1) = \sum_{i=1}^{m-2} i = \frac{(m-1)(m-2)}{2} = \frac{m^2 - 3m + 2}{2}. \end{aligned}$$

Anmerkung. Man sieht leicht, daß

$$\sum_{j=2}^{m-1} (m \bmod j) = \sum_{j=1}^m (m \bmod j) = m^2 - \sum_{j=1}^m \sigma(j)$$

mit der Teilersummen-Funktion σ . Aus [5, Satz 324] entnimmt man, dass sich diese letztere Summe asymptotisch wie $\frac{\pi^2}{12} \cdot m$ verhält, so dass man für $\sum (m \bmod j)$ asymptotisch die etwas bessere obere Schranke $0.18 \cdot m^2$ bekommt.

Korollar 1 *Unter den Voraussetzungen von Satz 7 gilt*

$$\frac{1}{2}p \cdot (p-1) \cdot \left(\ln \frac{p}{2} - 2\right) \leq l_2(p) \leq \frac{(p-1)(p-2)(p-3)}{4} + \frac{p \cdot (p-1)}{2} \cdot \ln(p-1).$$

Problem. Die obere Schranke $O(p^3)$ entstand durch sehr grobe Abschätzung. Die empirischen Ergebnisse zeigen eine deutliche Tendenz zur unteren Schranke. Gilt $l_2(m) = O(m^2 \cdot \ln m)$?

6 Anwendungen in der Invariantentheorie

Sei K ein Körper, der eine primitive m -te Einheitswurzel enthält, insbesondere $\text{char } K \nmid m$. Dann ist jede Darstellung der zyklischen Gruppe $G = Z_m$ diagonalisierbar: Sei $A \in Z_m$ ein erzeugendes Element und $\zeta \in K$ eine fest gewählte primitive m -te Einheitswurzel; es gibt dann eine Basis mit zugehörigen Koordinatenfunktionen X_1, \dots, X_n , so dass die induzierte Operation von Z_m auf dem Polynomring $K[X] = K[X_1, \dots, X_n]$ durch die Formeln

$$(Op) \quad A \cdot X_i = \zeta^{a_i} X_i$$

mit geeigneten $a_i \in \mathbb{Z}$, o. B. d. A. $0 \leq a_i \leq m-1$ für $i = 1, \dots, n$, gegeben ist. Ein Polynom $f = \sum_{\nu \in \mathbb{N}^n} c_\nu X^\nu$ ist genau dann invariant, wenn nur Monome mit $a_1 \nu_1 + \dots + a_n \nu_n \equiv 0 \pmod{m}$ vorkommen. Ein minimales Erzeugendensystem der Invarianten-Algebra $K[X]^G$ besteht also genau aus den Monomen X^ν , für die $\nu \in \mathbb{N}^n$ eine unzerlegbare Lösung der linearen Kongruenz (A) ist. Wohlbekannt und nicht besonders schwer zu zeigen ist:

Hilfssatz 6 *Sei R ein kommutativer Ring, A eine \mathbb{N}^n -graduierte R -Algebra und B eine homogene Unteralgebra von A . Sei p_1, \dots, p_m ein Erzeugendensystem von B . Dann gibt es unter den homogenen Bestandteilen der p_i auch m Stück q_1, \dots, q_m , die B erzeugen.*

Das bedeutet, dass das genannte minimale Erzeugendensystem von $K[X]^G$ sogar ein Erzeugendensystem minimaler Länge ist; seine Elementanzahl ist also die „Einbettungsdimension“ von $K[X]^G$. Damit hat die Lösung der Kongruenz (A) eine unmittelbare invariantentheoretische Deutung; insbesondere gilt:

Satz 8 *Die zyklische Gruppe $G = Z_m$ operiere auf dem Polynomring $K[X]$ wie in (Op). Dann ist die Einbettungsdimension der Invarianten-Algebra $K[X]^G$ gleich der Anzahl der unzerlegbaren Lösungen der Kongruenz (A).*

Aussagen über diese Anzahl stehen im Korollar zu Satz 1 und in Abschnitt 2. Diese Zahl lässt sich geometrisch deuten als Einbettungsdimension der Quotientensingularität K^n/G in 0 [12].

Es gibt aber auch noch eine indirekte, weiterreichende Anwendung in der Invariantentheorie. Hierzu sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Sei G eine reductive algebraische Gruppe und V ein endlich-dimensionaler G -Modul. Gegeben sei ein Punkt $v \in V$ mit abgeschlossener Bahn $G \cdot v$ und (daher) reaktivem Stabilisator H . Dann ist $V \cong T_v(G \cdot v) \oplus W$ als H -Modul mit dem „Scheibenraum“ W . Eine Folge von Lunas Satz von der etalen Scheibe ist, dass die Einbettungsdimension der Invarianten-Algebra von V unter G mindestens so groß ist wie die von W unter H [7, §2.5]. Für den Fall, dass $H \cong Z_m$, erhält man also für diese Einbettungsdimension eine Abschätzung nach unten.

Beispiel. Sei I_d die Invarianten-Algebra für die $(d + 1)$ -dimensionale Darstellung von $\mathbb{S}\mathbb{L}_2$ auf dem Raum R_d der binären Formen vom Grad d . Sei e_d ihre Einbettungsdimension. Bekannt ist für ungerade d , vgl. [7, §2.8]:

$$e_3 = 1, \quad e_5 = 4, \quad 28 \leq e_7 \leq 33.$$

Leicht zu sehen ist durch Angabe eines geeigneten Elements v , nämlich $v = X^{d-1}Y + XY^{d-1}$:

Satz 9 *Für ungerades $d \geq 3$ gilt $e_d \geq 1 + l(d - 2)$.*

Aus der Tabelle in Abschnitt 3 folgt:

Korollar 1 $e_9 \geq 48, e_{11} \geq 119, e_{13} \geq 328$.

Korollar 2 *Für ungerades $d \geq 9$ ist $e_d \geq 2 \cdot p(d - 2)$, insbesondere wächst e_d mindestens schwach exponentiell mit d .*

Bemerkung. Ebenso kann man für ungerades d die Einbettungsdimension e_d durch Wahl von $v = X^d + Y^d$ nach unten abschätzen durch die Anzahl der unzerlegbaren Lösungen der Kongruenz

$$\sum_{i \in I} ix_i \equiv 0 \pmod{d} \quad \text{mit} \quad I = \{0, \dots, d - 1\} - \{2, d - 2\}.$$

Daraus ergibt sich die Verschärfung $e_{11} \geq 164$.

Analoge Ergebnisse für gerades d erhält man aus der Untersuchung der homogenen linearen Gleichung (1), die ich in einer folgenden Arbeit behandeln will. Die Aufgabe, die Invarianten der binären Formen vom Grad d zu bestimmen, hat also eine exponentielle Komplexität und darf daher als undurchführbar angesehen werden (solange nicht durch neue theoretische Erkenntnisse ein besserer Überblick ermöglicht wird, was ich aber für völlig unwahrscheinlich halte). Auch die unteren Grenzen für die ersten unbekanntesten Fälle, $e_9 \geq 48, e_{10} \geq 44, e_{12} \geq 52$ (im Vorgriff), $e_d \geq 100$ für $d \geq 11$ sonst, zeigen, dass die Invariantentheorie des 19. Jahrhunderts bei dieser Aufgabe schon bis an die Grenzen des (auch heute) Machbaren vorgedrungen ist.

Literatur

- [1] P. Bachmann: *Niedere Zahlentheorie*, Zweiter Teil, Additive Zahlentheorie. Teubner Leipzig 1910.
- [2] L. E. Dickson: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Amer. J. Math.* 35 (1913), 413–422.
- [3] E. Ehrhardt: Sur un problème de géométrie diophantienne. *J. reine angew. Math.* 226 (1967), 1–29; 227 (1967), 25–49; 231 (1968), 220.
- [4] E. Ehrhardt: Sur les équations diophantiennes linéaires. *C. R. Acad. Sc. Paris* 288 (1979), Série A, 785–787.
- [5] G. H. Hardy, E. M. Wright: *Zahlentheorie*. Oldenbourg, München 1958. = *Introduction to the Theory of Numbers*. Oxford Univ. Press 1938, 1954.
- [6] G. Hochschild: ??
- [7] V. G. Kac: Root systems, representations of quivers and invariant theory. *Invariant Theory*, Montecatini 1982, ed. by F. Gherardelli. Springer Lect. Notes 996 (1983).
- [8] D. Knuth: *The Art of Computer Programming*, Volume 1, Fundamental Algorithms. Addison-Wesley, Reading Mass. 1968, 1973.
- [9] H. Ostmann: *Additive Zahlentheorie*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, Berlin usw. 1956.
- [10] L. Rédei: *Theorie der endlich erzeugbaren kommutativen Halbgruppen*. Akadémiai Kiadó, Budapest 1963.
- [11] *Reviews in Number Theory*. Ed. by W. J. LeVeque. Amer. Math. Soc., Providence R.I. 1974.
- [12] O. Riemenschneider: Deformationen von Quotientensingularitäten (nach zyklischen Gruppen). *Math. Ann.* 209 (1974), 211–248.
- [13] O. Riemenschneider: Die Invarianten der endlichen Untergruppen von $GL(2, \mathbb{C})$. *Math. Z.* 153 (1977), 37–50.
- [14] M. F. Tinsley: Permanents of cyclic matrices. *Pacific J. Math.* 10 (1960), 1067–1082.
- [15] M. F. Tinsley: A combinatorial theorem in number theory. *Duke Math. J.* 33 (1966), 75–79.