Eine einheitliche Methode zur Behandlung einer linearen Kongruenz mit Nebenbedingungen

Autor(en): **Spilker, Jürgen**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **51 (1996)**

PDF erstellt am: **24.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-46963

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

El. Math. *51* (1996)

0013-6018/96/020107-10$1.50 + 0.20/0
© 1996 Birkhäuser Verlag, Basel

Eine einheitliche Methode zur Behandlung einer linearen Kongruenz mit Nebenbedingungen

Jürgen Spilker

Jürgen Spilker wurde 1935 geboren. Er studierte und promovierte in Göttingen und ist seit 1970 Professor für Mathematik an der Universität Freiburg (Breisgau). Sein wissenschaftliches Interesse galt zunächst den automorphen Formen, heute der elementaren Zahlentheorie, insbesondere den arithmetischen Funktionen.

Seien n und r natürliche Zahlen. Man nennt

$$x_1 + x_2 + \cdots + x_s \equiv n \pmod{r} \tag{1}$$

eine lineare Kongruenz in s Veränderlichen zum Modul r. Eine Lösung ist ein s-Tupel ganzer Zahlen $x_1, x_2, \ldots, x_s$, wobei 2 Lösungstupel als gleich angesehen werden, wenn ihre Komponenten modulo r gleich sind. Die Kongruenz (1) hat offenbar r^{s-1} Lösungen.

In der elementaren Zahlentheorie bestimmt man Anzahlen von Lösungen der Kongruenz (1), welche Nebenbedingungen unterliegen, z.B. größter gemeinsamer Teiler $(x_i, r) = 1$ für $1 \leq i \leq s$. Diese Anzahlen sind in vielen Arbeiten behandelt worden. Eine zusammenfassende Darstellung findet man in [4], Kap. 3. In diesem Aufsatz wird eine einheitliche Methode zur Bestimmung derartiger Anzahlen vorgestellt:

- die Anzahlen sind das Cauchy-Produkt von einfachen Grundfunktionen;
- die Grundfunktionen sind arithmetische Funktionen in 2 Variabeln, welche in der ersten Veränderlichen r-gerade und in der anderen multiplikativ sind;
- diese Eigenschaften bleiben beim Cauchy-Produkt erhalten und führen somit direkt zu Ramanujan-Entwicklungen und Produktdarstellungen der Lösungsanzahlen; aus diesen erkennt man z.B., wann eine Kongruenz (1) mit Nebenbedingungen lösbar ist und wann nicht.

Gegeben ist eine lineare Kongruenz $x_1 + x_2 + \cdots + x_s \equiv n \pmod{r}$ und für jedes i, $1 \leq i \leq s$, ein Teiler d_i von r. Wieviele Lösungen modulo r der Kongruenz gibt es, welche der Nebenbedingung $(x_i, r) = d_i$, $1 \leq i \leq s$, genügen? Diese häufig auftretende Frage führt auf interessante zahlentheoretische Probleme. In der vorliegenden Arbeit wird ein Verfahren angegeben, mit dessen Hilfe sich diese Anzahl auf eine einheitliche Weise bestimmen lässt. *ust*

1 r-gerade Funktionen und Ramanujan-Entwicklungen

Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt *r-gerade* ($r \in \mathbb{N}$), wenn

$$f(n) = f((n,r)) \text{ für alle } n \in \mathbb{N}$$

gilt. Eine derartige Funktion ist also durch ihre Werte auf allen Teilern von r bestimmt. Typische r-gerade Funktionen sind die *Ramanujan-Summen*

$$c(n,r) := \sum_{\substack{1 \le x \le r \\ (x,r)=1}} e^{2\pi i\, nx/r}.$$

Weil die Funktionen $n \mapsto c(n,d)$ für $d|r$ r-gerade und linear unabhängig sind und die Dimension des komplexen Vektorraumes aller r-geraden Funktionen gleich der Teileranzahl von r ist, gilt

Satz 1 ([6], S. 124). *Für jedes natürliche r bilden die Ramanujan-Summen*

$$c(\cdot,d) \text{ mit } d|r$$

eine Basis des Vektorraumes der r-geraden Funktionen.

Jede r-gerade Funktion f hat folglich eine Entwicklung

$$f(n) = \sum_{d|r} a(d,r)c(n,d)$$

mit eindeutig bestimmten komplexen "Ramanujan-Koeffizienten"

$$a(d,r) = \frac{1}{r}\sum_{e|r} f\left(\frac{r}{e}\right) c\left(\frac{r}{d},e\right), \quad d|r.$$

Diese Formel erhält man aus den für alle Teiler t_1, t_2 von r gültigen Orthogonalitätsrelationen ([4], S. 78)

$$\sum_{d|r} c\left(\frac{r}{d},t_1\right) c\left(\frac{r}{t_2},d\right) = \begin{cases} 0 & \text{falls } t_1 \neq t_2, \\ r & \text{sonst,} \end{cases} \tag{2}$$

denn es gilt

$$\begin{aligned}
\sum_{d|r} a(d,r)c(n,d) &= \sum_{d|r} \frac{1}{r} \sum_{e|r} f\left(\frac{r}{e}\right) c\left(\frac{r}{d},e\right) c(n,d) \\
&= \frac{1}{r}\sum_{e|r} f(e) \sum_{d|r} c\left(\frac{r}{d},\frac{r}{e}\right) c((n,r),d) \\
&= f((n,r)) \\
&= f(n),
\end{aligned}$$

weil die innere Summe nach (2) für $e \neq (n,r)$ verschwindet und sonst den Wert r hat. Also gilt der

Satz 2 ([4], S. 80). *Jede r-gerade Funktion f hat eine Darstellung*

$$f = \sum_{d|r} a(d,r)c(\cdot,d).$$

Die Koeffizienten sind eindeutig bestimmt und berechnen sich aus

$$a(d,r) = \frac{1}{r}\sum_{e|r} f\left(\frac{r}{e}\right) c\left(\frac{r}{d},e\right), \quad d|r. \tag{3}$$

Beispiele:

1. Für jedes natürliche r ist die Funktion

$$n \mapsto f(n,r) := \begin{cases} 1 & \text{falls } (n,r) = 1, \\ 0 & \text{sonst} \end{cases}$$

r-gerade mit Ramanujan-Koeffizienten

$$a(d,r) = \frac{1}{r}c\left(\frac{r}{d},r\right) = \frac{\mu(d)\varphi(r)}{r\varphi(d)}, \quad d|r.$$

2. Seien r und k natürliche Zahlen und

$$g_k(n,r) := \begin{cases} 1 & \text{falls } (n,r) \text{ eine } k\text{-te Potenz ist,} \\ 0 & \text{sonst.} \end{cases}$$

Die Funktion $g_k(\cdot,r)$ ist r-gerade und

$$a(d,r) = \frac{1}{r}\sum_{e^k|r} c\left(\frac{r}{d},\frac{r}{e^k}\right), \quad d|r.$$

Mit der Funktion $\lambda_k(n) := \sum_{d^k|r} \mu\left(\frac{n}{d^k}\right)$ wird ([2], S. 21)

$$a(d,r) = \frac{1}{r}\sum_{t|\frac{r}{d}} t\lambda_k\left(\frac{r}{t}\right).$$

3. Seien r und k natürliche Zahlen und

$$h_k(n,r) := \begin{cases} 1 & \text{falls } (n,r)\ k\text{-frei ist,} \\ 0 & \text{sonst.} \end{cases}$$

Dabei heißt eine natürliche Zahl a k-frei, wenn $d^k|a$ für kein $d > 1$ gilt. Die Funktionen $h_k(\cdot,r)$ sind r-gerade und

$$a(d,r) = \frac{1}{r}\sum_{\substack{e|r \\ (e,r)_k=1}} c\left(\frac{r}{d},\frac{r}{e}\right), \quad d|r;$$

dabei bezeichnet $(e,r)_k$ den größten gemeinsamen Teiler von e und r, der eine k-Potenz ist. Auch dieser Wert ist in [2], S. 21 berechnet worden, und zwar mittels $\mu_k(n) := \sum_{\substack{d|n \\ (d,n)_k=1}} \mu\left(\frac{r}{d}\right)$ zu

$$a(d,r) = \frac{1}{r}\sum_{t|\frac{r}{d}} t\mu_k\left(\frac{r}{t}\right).$$

2 Cauchy-Produkt und Multiplikativität

Von je zwei arithmetischen Funktionen f, g kann man das *Cauchy-Produkt*

$$(f \odot g)(n) := \sum_{\substack{1 \le x,y \le r \\ x+y \equiv n (\mathrm{mod}\, r)}} f(x)g(y)$$

bilden. Es ist assoziativ und kommutativ. Aus den Orthogonalitätsrelationen ([4], S. 76)

$$\sum_{\substack{1 \le x,y \le r \\ x+y \equiv n (\mathrm{mod}\, r)}} c(x,t_1)c(y,t_2) = \begin{cases} 0 & t_1 \neq t_2 \\ rc(n,t_1) & t_1 = t_2, \end{cases}$$

welche für alle Teiler t_1, t_2 von r gelten, folgt, daß für zwei r-gerade Funktionen f, g auch $f \odot g$ r-gerade ist und gilt

Satz 3 ([4], S. 84). *Sind f und g r-gerade Funktionen mit Ramanujan-Koeffizienten $a(d,r)$ bzw. $b(d,r)$, $d|r$, dann hat das Cauchy-Produkt $f \odot g$ die Ramanujan-Koeffizienten $ra(d,r)b(d,r)$, $d|r$.*

Bei arithmetischen Funktionen in zwei Veränderlichen gibt es einen zweifachen Zusammenhang von Ramanujan-Koeffizienten in der einen und Multiplikativität in der anderen.

Satz 4. *Sei $f : \mathbb{N} \times \mathbb{N} \to \mathbb{C}$ eine Funktion, und für jedes natürliche r sei $n \mapsto f(n,r)$ eine r-gerade Funktion; ihre Ramanujan-Entwicklung laute*

$$f(n,r) = \sum_{d|r} a(d,r)c(n,d), \qquad n \in \mathbb{N}.$$

Dann sind die folgenden beiden Eigenschaften äquivalent:

(4) $r \to f(n,r)$ *ist multiplikativ für jedes natürliche n;*

(5) $\begin{cases} a(d_1d_2, r_1r_2) = a(d_1,r_1)a(d_2,r_2), & \textit{falls } d_1|r_1,\ d_2|r_2, (r_1,r_2) = 1; \\ \textit{insbesondere } a(1,1) = 1. \end{cases}$

Beweis: (4) $\Rightarrow$ (5): Sei gegeben $(r_1,r_2) = 1$, $d_1|r_1, d_2|r_2$. Wegen (3) gilt

$$\begin{aligned} a(d_1d_2, r_1r_2) &= \frac{1}{r_1r_2} \sum_{e|r_1r_2} f\left(\frac{r_1r_2}{e}, r_1r_2\right) c\left(\frac{r_1r_2}{d_1d_2}, e\right) \\ &= \frac{1}{r_1} \cdot \frac{1}{r_2} \sum_{e_1|r_1} \sum_{e_2|r_2} f\left(\frac{r_1}{e_1}\frac{r_2}{e_2}, r_1r_2\right) c\left(\frac{r_1}{d_1}\frac{r_2}{d_2}, e_1e_2\right). \end{aligned}$$

Der f-Wert zerfällt wegen (4) in

$$f\left(\frac{r_1}{e_1}\frac{r_2}{e_2}, r_1\right) f\left(\frac{r_1}{e_1}\frac{r_2}{e_2}, r_2\right) = f\left(\frac{r_1}{e_1}, r_1\right) f\left(\frac{r_2}{e_2}, r_2\right).$$

In analoger Weise kann man die Ramanujan-Summe zerlegen ([4], S. 89, Exercise 2.2). Man erhält

$$\begin{aligned} a(d_1d_2, r_1r_2) &= \prod_{i=1}^{2} \frac{1}{r_i} \sum_{e_i|r_i} f\left(\frac{r_i}{e_i}, r_i\right) c\left(\frac{r_i}{d_i}, e_i\right) \\ &= a(d_1, r_1)a(d_2, r_2). \end{aligned}$$

Ferner gilt

$$1 = f(1,1) = a(1,1)c(1,1) = a(1,1).$$

(5) $\Rightarrow$ (4): Sei $n \in \mathbb{N}$, $(r_1, r_2) = 1$ gegeben. Es gilt

$$\begin{aligned} f(n, r_1r_2) &= \sum_{d|r_1r_2} a(d, r_1r_2)c(n,d), \\ &= \sum_{d_1|r_1} \sum_{d_2|r_2} a(d_1d_2, r_1r_2)c(n, d_1d_2). \end{aligned}$$

Der Ramanujan-Koeffizient zerfällt nach (5), und $d \mapsto c(n,d)$ ist multiplikativ ([6], S. 16). Es folgt

$$f(n, r_1r_2) = \prod_{i=1}^{2} \sum_{d_i|r_i} a(d_i, r_i)c(n, d_i) = f(n, r_1)f(n, r_2).$$

Letztlich ist

$$f(n,1) = a(1,1)c(n,1) = 1,$$

also ist $f(n, \cdot)$ multiplikativ. □

Aus den letzten beiden Sätzen folgt der für unsere Anwendungen wichtige

Satz 5. *Sind $f_i(n,r)$ komplexwertige Funktionen auf $\mathbb{N} \times \mathbb{N}$, $1 \le i \le s$, und ist $F(n,r)$ ihr Cauchy-Produkt bzgl. der ersten Veränderlichen, dann gilt:*

a) Sind für jedes natürliche r die Funktionen

$$n \mapsto f_i(n,r), \qquad 1 \le i \le s$$

r-gerade mit Ramanujan-Koeffizienten $a_i(d,r)$, $d|r$, dann hat $F(\cdot, r)$ die Ramanujan-Koeffizienten

$$r^{s-1} \prod_{i=1}^{s} a_i(d,r), \qquad d|r;$$

b) Sind zusätzlich für jedes natürliche n die Funktionen

$$r \mapsto f_i(n,r), \qquad 1 \le i \le s$$

multiplikativ, dann ist auch $F(n, \cdot)$ multiplikativ für alle n, und es gilt

$$\begin{aligned} F(n,r) &= \prod_{p^\alpha \| r} F(n, p^\alpha) \\ &= \prod_{p^\alpha \| r} F(p^{\min\{\alpha,\beta\}}, p^\alpha), \end{aligned}$$

wobei $p^\beta \| n$.

3 Anwendung auf lineare Kongruenzen

Wir betrachten jetzt die lineare Kongruenz

$$x_1 + x_2 + \cdots + x_s \equiv n \pmod{r} \tag{1}$$

unter verschiedenen Nebenbedingungen; dabei sind n, r, s natürliche Zahlen. Die Lösungsanzahlen sind das Cauchy-Produkt von einfachen Grundfunktionen in 2 Variablen n, r, welche in n r-gerade und in r multiplikativ sind. Mit Satz 5 ergeben sich sofort die Ramanujan-Entwicklung sowie eine Produktdarstellung.

1. Zunächst betrachten wir alle Lösungen, deren Komponenten zu r teilerfremd sind. Wir betrachten also

$$N(n,r,s) := \#\{(x_1,\ldots,x_s) \text{ Lösung von (1): } 1 \le x_i \le r,\ (x_i,r) = 1 \text{ für } 1 \le i \le s\}\,.$$

Es ist

$$\begin{aligned} N(n,r,s) &= \sum_{\substack{x_s+y\equiv n \pmod r\\ (x_s,r)=1}} \ \sum_{\substack{x_1+\cdots+x_{s-1}\equiv y \pmod r\\ (x_i,r)=1}} 1 \\ &= \sum_{\substack{x_s+y\equiv n \pmod r\\ (x_s,r)=1}} N(y,r,s-1) \\ &= f(\cdot,r) \odot N(\cdot,r,s-1) \end{aligned}$$

mit der Funktion $f(\cdot,r)$ aus Abschnitt 1, Beispiel 1. Wegen $N(n,r,1) = f(n,r)$ ist $N(\cdot,r,s)$ das s-fache Cauchy-Produkt von $f(\cdot,r)$ mit sich selbst. Da $f(\cdot,r)$ r-gerade und $f(n,\cdot)$ multiplikativ ist, ergibt Satz 5 direkt die Darstellung ([4], S. 117)

$$\begin{aligned} N(n,r,s) &= \frac{1}{r}\sum_{d|r} c\left(\frac{r}{d},r\right)^s c(n,d) \\ &= \frac{\varphi(r)^s}{r}\sum_{d|r}\frac{\mu(d)^s}{\varphi(d)^s}c(n,d) \end{aligned} \tag{6}$$

sowie die Produktformel ([4], S. 118)

$$N(n,r,s) = \prod_{p^\alpha \| r} N(n,p^\alpha,s).$$

Die Faktoren berechnen sich aus (6) zu ([4], S. 119)

$$N(n,p^\alpha,s) = \begin{cases} p^{\alpha(s-1)}\,\frac{(p-1)\,((p-1)^{s-1}-(-1)^{s-1})}{p^s} & p|n, \\ p^{\alpha(s-1)}\,\frac{(p-1)^s-(-1)^s}{p^s} & p\nmid n. \end{cases}$$

Hieraus ergibt sich: (1) hat genau dann keine Lösung mit $(x_i,r) = 1$, wenn einer der drei folgenden Fälle vorliegt:

- $(n,r) > 1$, $s = 1$;
- n, r gerade, s ungerade;
- n ungerade, r, s gerade.

2. Sei $P_k(n,r,s)$ die Anzahl der Lösungen modulo r von (1), die den Bedingungen

$$(x_i, r) \text{ ist eine } k\text{-te Potenz}, \ 1 \le i \le s$$

genügen. Diese Anzahl ist das s-fache Cauchy-Produkt der Funktion $g_k(\cdot, r)$ aus Abschnitt 1, Beispiel 2, und $g_k(\cdot, r)$ ist r-gerade und $g_k(n, \cdot)$ multiplikativ. Satz 5 ergibt

$$P_k(n,r,s) = \frac{1}{r} \sum_{d|r} \left(\sum_{e^k|r} c\left(\frac{r}{d}, \frac{r}{e^k}\right) \right)^s c(n,d)$$

und

$$P_k(n,r,s) = \prod_{p^\alpha \| r} P_k(n, p^\alpha, s).$$

Für $P_k(n, p^\alpha, s)$ scheint keine explizite Formel bekannt zu sein.

3. Eine verwandte Lösungszahl ist $Q_k(n,r,s)$, die Anzahl der Lösungen mod r von (1), die den Bedingungen

$$(x_i, r) \text{ ist } k\text{-frei}, \ 1 \le i \le s$$

genügen. Die Anzahl ist das s-fache Cauchy-Produkt der Funktion $h_k(\cdot, r)$ (siehe Abschnitt 1, Beispiel 3). Nach Satz 5 ist

$$Q_k(n,r,s) = \frac{1}{r} \sum_{d|r} \left(\sum_{\substack{e|r \\ (e,r)_k = 1}} c\left(\frac{r}{d}, \frac{r}{e}\right) \right)^s c(n,d)$$

sowie

$$Q_k(n,r,s) = \prod_{p^\alpha \| r} Q_k(n, p^\alpha, s).$$

Man berechnet ([5], S. 72)

$$Q_k(n,p^\alpha,s) = \begin{cases} p^{\alpha(s-1)} & \alpha < k, \\ p^{\alpha(s-1)} \frac{(p^k-1)[(p^k-1)^{s-1}-(-1)^{s-1}]}{p^{ks}} & \alpha \ge k,\ p^k | n, \\ p^{\alpha(s-1)} \frac{(p-1)^s-(-1)^s}{p^{ks}} & \alpha \ge k,\ p^k \nmid n. \end{cases}$$

Es gilt $Q_k(n,r,s) = 0$ genau dann, wenn

- $(n,r)_k = 1$, $s = 1$,
- oder $k = 1$, n, r gerade, s ungerade,
- oder $k = 1$, n ungerade, r, s gerade.

4. Man kann auch Mischungen obiger Nebenbedingungen behandeln. Ein bekanntes Beispiel ([2], S. 22) ist die Anzahl $\varepsilon_k(n,r)$ der Lösungen mod r von $x_1+x_2 \equiv n \pmod r$ mit

$$(x_1,r)=1, \quad (x_2,r) \text{ ist } k\text{-Potenz.}$$

Es gilt

$$\varepsilon_k(\cdot,r) = f(\cdot,r) \odot g_k(\cdot,r)$$

und folglich

$$\varepsilon_k(n,r) = \frac{1}{r}\sum_{d|r} c\left(\frac{r}{d},r\right) \sum_{e^k|r} c\left(\frac{r}{d},\frac{r}{e^k}\right) c(n,d)$$

und

$$\varepsilon_k(n,r) = \prod_{p^\alpha \| r} \varepsilon_k(n,p^\alpha).$$

Die Faktoren berechnen sich zu ([2], S. 22)

$$(p^k-1)\varepsilon_k(n,p^\alpha) = \begin{cases} p^{\alpha-1}(p-1)(p^k-1) & p|n, \\ p^{\alpha+k-1}(p-2)+p^{\alpha-1}+p^{k-1}-1 & p\nmid n,\ k|\alpha, \\ p^{\alpha+k-1}(p-2)+p^{\alpha-1}-p^{t-1}(p-1) & p\nmid n,\ k\nmid\alpha, \end{cases}$$

dabei ist im 3. Fall t bestimmt durch $\alpha \equiv t \pmod k$, $1 \le t \le k-1$. Nur in diesem Fall kann $\varepsilon_k(n,p^\alpha)=0$ sein.

Es folgt

$$\varepsilon_k(n,r)=0 \Leftrightarrow n \text{ ungerade, } 2|r, 2^k\nmid r.$$

5. Eine allgemeine Beispielklasse erhält man, indem man für $i \in \{1,2,\dots,s\}$ nichtleere Mengen $D_i(r)$ von Teilern von r vorgibt und die Anzahl $M(n,r,s)$ der Lösungen $(x_1,\dots,x_s)$ modulo r von (1) mit

$$(x_i,r) \in D_i(r), \qquad 1 \le i \le s$$

eingeführt ([4], S. 121). Mit den Grundfunktionen

$$d_i(n,r) := \begin{cases} 1 & (n,r) \in D_i(r) \\ 0 & \text{sonst} \end{cases}$$

wird $M(\cdot,r,s) = d_s \odot d_{s-1} \odot \cdots \odot d_1(\cdot,r)$, und Satz 5a) ergibt ([3], S. 121)

$$M(n,r,s) = \frac{1}{r}\sum_{d|r}\prod_{i=1}^{s}\sum_{\substack{e|r \\ e\in D_i(r)}} c\left(\frac{r}{d},\frac{r}{e}\right) c(n,d).$$

Wenn für alle teilerfremden Paare (r_1,r_2) und alle i die Eigenschaft

$$d_1 \in D_i(r_1),\ d_2 \in D_i(r_2) \ \Leftrightarrow\ d_1d_2 \in D_i(r_1r_2)$$

gilt, dann sind alle Funktionen $d_i(n,\cdot)$ multiplikativ, und nach Satz 5b) gilt

$$M(n,r,s) = \prod_{p^\alpha \| r} M(p^{\min\{\alpha,\beta\}}, p^\alpha, s)\ ,$$

wobei $p^\beta \| n$. Die Beispiele 1 bis 4 sind Spezialfälle hiervon.

6. Zuletzt werden noch zwei weitere Beispiele angegeben, die sich dem allgemeinen Fall 5 unterordnen:

a) $s = 2$, $(x_1, r) = 1$, $(x_2, r)_k = 1$; die zugehörigen Lösungszahlen $\Theta_k(n,r)$ wurden in [2], S. 22 behandelt; $\Theta_1(n,r) = N(n,r,2)$ ist die Nagell-Funktion ([4], S. 119).

b) Seien a_i $(1 \le i \le s)$ ganze Zahlen und sei $A(n,r,s)$ die Anzahl der Lösungen $\bmod r$ von

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s \equiv n \pmod r \text{ mit } (x_i, r) = 1.$$

Dann gilt ([1] Cor. 1.12)

$$A(n,r,s) = \frac{1}{r}\sum_{d|r}\prod_{i=1}^{s} c\left(\frac{r}{d}, \frac{r}{d_i}\right) c(n,d) \prod_{i=1}^{s} \frac{\varphi(r)}{\varphi(\frac{r}{d_i})}$$

mit $d_i := (a_i, r)$.

Der *Beweis* folgt aus:

(i) die Anzahl der Lösungen $\bmod r$ von

$$y_1 + y_2 + \cdots + y_s \equiv n \pmod r \text{ mit } (y_i, r) = d_i$$

ist

$$M(n,r,s) = \frac{1}{r}\sum_{d|r}\prod_{i=1}^{s} c\left(\frac{r}{d}, \frac{r}{d_i}\right) c(n,d);$$

(ii) $\#\{1 \le x \le r\colon ax \equiv y \bmod r,\ (x,r) = 1\} = \frac{\varphi(r)}{\varphi(\frac{r}{d})}$, sofern $(a,r) = (y,r) = d$.

Die Aussage in (i) ist ein Spezialfall von Beispiel 5 ($D_i(r) = \{d_i\}$, s.a. [4], S. 138, Exercise 3.8).

Zur Aussage (ii) bemerken wir, dass der Reduktionshomomorphismus der primen Restklassengruppen

$$f_1 : \mathbb{Z}_r^* \to \mathbb{Z}_{r/d}^* : x \bmod r \mapsto x \bmod \frac{r}{d}$$

surjektiv ist und

$$f_2 : \mathbb{Z}_{r/d}^* \to \mathbb{Z}_{r/d}^* : x \bmod \frac{r}{d} \mapsto \frac{a}{d}x \bmod \frac{r}{d}$$

bijektiv ist; also hat jedes Element von $\mathbb{Z}_{r/d}^*$ unter der Abbildung $f_2 \circ f_1$ genau soviele Urbilder, wie es Elemente im Kern von f_1 gibt, also $\varphi(r)/\varphi(\frac{r}{d})$.

Literatur

[1] U. Cerruti: Counting the Number of Solutions of Congruences. E. Bergum et al (eds.), Applications of Fibonacci Numbers, vol. 5, 85–101, Kluwer Acad. Publ. 1993.

[2] E. Cohen: A class of residue systems $(\bmod r)$ and related arithmetical functions. I. A generalization of Möbius inversion. Pacific J. Math. 9 (1959), 13–23.

[3] P. Haukanen and R. Sivaramakrishnan: Cauchy multiplication and periodic functions $(\bmod r)$. Collect. Math. 42 (1991), 33–44.

[4] P.J. McCarthy: Introduction to Arithmetical Functions. Springer, New York, 1986.

[5] A. Metzger: Lineare Kongruenzen und Cauchy-Operatoren, Staatsarbeit, Freiburg, 1994.

[6] W. Schwarz and J. Spilker: Arithmetical Functions, Cambridge University Press, 1994.

Jürgen Spilker
Math. Institut der Universität
Eckerstr. 1
D-79104 Freiburg