Über vollständig q-additive Funktionen und die Primfaktorzerlegung von $n!$

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz
Universität Hannover
zur Erlangung des Grades
Doktorin der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation

von

Dipl.-Math. Iris Lieske
geboren am 23. Februar 1978 in Höxter

2007

Referent:	Prof. Dr. J. Sander
Korreferent:	Prof. Dr. C. Elsner
Tag der Promotion:	13. Juli 2007

Zusammenfassung

Diese Arbeit beschäftigt sich mit den vollständig q-additiven Funktionen sowie der Primfaktorzerlegung von $n!$.

Sei q eine ganze Zahl mit $q \geq 2$. Eine Funktion $f : \mathbb{N}_0 \to \mathbb{C}$ nennt man vollständig q-additiv, falls $f(0) = 0$ und $f(aq^k+b) = f(a)+f(b)$ für alle ganzen Zahlen $a \geq 1$, $k \geq 1$ und $0 \leq b < q^k$ gilt. In dieser Arbeit wird gezeigt, dass die Zahlen $\mathbf{f}(\mathbf{u}n + \mathbf{v})$, wobei $\mathbf{f} = (f_1, \ldots, f_l)$, die f_i vollständig q_i-additive Funktionen mit ganzzahligen Werten und $\mathbf{u}$ und $\mathbf{v}$ l-Tupel aus ganzen Zahlen mit bestimmtem Eigenschaften seien, auf den Restklassen modulo $(m_1, \ldots, m_l)$ gleichverteilt sind. Dies stellt eine Verallgemeinerung eines Satzes von Kim (J. Number Theory 102 (2003), 298-305) dar.

Dieses Resultat wird verwendet, um zu zeigen, dass für feste Primzahlen $p_1, \ldots, p_l$ und für feste ganze Zahlen $m_1, \ldots, m_l$ mit $p_i \nmid m_i$ oder $m_i = p_i^{\alpha_i}$ mit $\alpha_i \geq 1$, die Zahlen $e_{p_1}(n!), \ldots, e_{p_l}(n!)$ auf den Restklassen modulo $(m_1, \ldots, m_l)$ gleichverteilt sind, wobei $e_{p_i}(n!)$ den Exponenten bezeichne, mit dem p_i in der Primfaktorzerlegung von $n!$ auftritt. Die Ziffernsumme $S_{p_i}(n)$ wird hierbei in ihrer Eigenschaft als vollständig p_i-additive Funktion verwendet. Somit wird eine allgemeinere Fassung einer Vermutung von Erdős und Graham (Monogr. Enseign. Math. 28 (1980), 128) gezeigt.

Schlagwörter: q-additive Funktion, Primfaktorzerlegung, Fakultät, Gleichverteilung.

Abstract

This thesis deals with completely q-additive functions and the prime factorization of $n!$.

Let q be an integer with $q \geq 2$. A function $f : \mathbb{N}_0 \to \mathbb{C}$ is called completely q-additive if $f(0) = 0$ and $f(aq^k + b) = f(a) + f(b)$ for any integers $a \geq 1$, $k \geq 1$, and $0 \leq b < q^k$. In this thesis it is shown that the numbers $\mathbf{f}(\mathbf{u}n+\mathbf{v})$, where $\mathbf{f} = (f_1, \ldots, f_l)$ and f_i are integer valued completely q_i-additive functions and $\mathbf{u}$ and $\mathbf{v}$ are l-tuples of integers with certain properties, is uniformly distributed in residue classes modulo $(m_1, \ldots, m_l)$. This is a generalization of Kim's result (J. Number Theory 102 (2003) 298-305).

This result is used to show that for fixed primes $p_1, \ldots, p_l$ and for fixed integers $m_1, \ldots, m_l$ with $p_i \nmid m_i$ or $m_i = p_i^{\alpha_i}$ with $\alpha_i \geq 1$, the numbers $e_{p_1}(n!), \ldots, e_{p_l}(n!)$ are uniformly distributed in residue classes modulo $(m_1, \ldots, m_l)$, where $e_{p_i}(n!)$ denotes the order of p_i in the prime factorization of $n!$. The sum of digits $S_{p_i}(n)$ is used here because it is a completely p_i-additive function with appropriate properties. Hence, a generalization of a conjecture of Erdős and Graham (Monogr. Enseign. Math. 28 (1980) 128) is shown.

Keywords: q-additive function, prime factorization, factorial, uniform distribution.

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Die q-additiven Funktionen und die Primfaktorzerlegung von n!

Sei q eine ganze Zahl mit $q \geq 2$. Eine Funktion $f : \mathbb{N}_0 \to \mathbb{C}$ nennt man q-additiv, falls $f(0) = 0$ und $f(aq^k + b) = f(aq^k) + f(b)$ für alle ganzen Zahlen $a \geq 0$, $k \geq 0$ und $0 \leq b < q^k$ gilt. Eine q-additive Funktion wird vollständig q-additiv genannt, falls sogar $f(aq^k + b) = f(a) + f(b)$ für alle ganze Zahlen $a \geq 1$, $k \geq 1$ und $0 \leq b < q^k$ gilt.

Die q-additiven Funktionen wurden 1967/1968 von Gelfond [10] eingeführt. Er bewies bereits einige Theoreme über die Ziffernsumme $S_q(n) = \sum_{j=0}^{s} n_j$, wobei $n = \sum_{j=0}^{s} n_j q^j$ die q-adische Entwicklung der positiven ganzen Zahl n sei. Bei der Ziffernsumme handelt es sich um die am meisten untersuchte vollständig q-additive Funktion. Delange [7], Bésineau [3], Coquet [6], Kàtai [13] und andere untersuchten die q-additiven Funktionen weiter. Insbesondere bewies Gelfond [10], dass für eine ganze Zahl m mit $m \geq 2$ und $(m, q-1) = 1$ die Funktion $S_q(n)$ auf den Restklassen modulo m gleichverteilt ist. Im Detail zeigte er, dass für ganze Zahlen a die Abschätzung

$$|\{0 \leq n < N : S_q(n) \equiv a \bmod m\}| = \frac{N}{m} + \mathcal{O}\left(N^{1-\delta}\right)$$

gilt, wobei δ eine positive Konstante ist, die nur von q und m abhängt. Außerdem regte er die Frage an, ob für beliebige ganze Zahlen a_1, a_2 und ganze Zahlen $m_1, m_2, q_1, q_2 \geq 2$

mit $(m_1, q_1 - 1) = 1$, $(m_2, q_2 - 1) = 1$ und $(q_1, q_2) = 1$ die Abschätzung

$$|\{0 \leq n < N : S_{q_1}(n) \equiv a_1 \bmod m_1,\ S_{q_2}(n) \equiv a_2 \bmod m_2\}| = \frac{N}{m_1 m_2} + \mathcal{O}\left(N^{1-\delta}\right)$$

gilt. Bésineau [3] bewies, dass die rechte Seite der Gleichung asymptotisch gleich $\frac{N}{m_1 m_2}$ ist, erhielt jedoch nicht den angeführten Fehlerterm. Noch allgemeiner bewies er, dass für ganze Zahlen $a_1, a_2, \ldots, a_l$

$$\left|\left\{0 \leq n < N : S_{q_j}(n) \equiv a_j \bmod m_j\ (1 \leq j \leq l)\right\}\right| \sim \frac{N}{m_1 \cdots m_l} \quad (N \to \infty)$$

gilt, wobei vorausgesetzt wurde, dass $(q_i, q_j) = 1$ $(i \neq j)$ und $(m_j, q_j - 1) = 1$ für $1 \leq j \leq l$ sind. Bésineau konstruierte hierfür eine so genannte pseudozufällige Folge in Abhängigkeit von S_{q_j} und schloss mit Hilfe des Gleichverteilungskriteriums von Weyl [21] die Aussage.

Kim [14] konnte schließlich die Aussage inklusive des Fehlerterms beweisen und sogar die Funktion S_{q_j} durch eine beliebige vollständig q-additive Funktion f_j ersetzen. Er bewies

$$|\{0 \leq n < N : f_j(n) \equiv a_j \bmod m_j\ (1 \leq j \leq l)\}| = \frac{N}{m_1 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right)$$

unter bestimmten Voraussetzungen, die aber bei der Ziffernsumme gegeben sind, falls $(m_j, q_j - 1) = 1$ ist. Diese Aussage fand zunächst direkte Anwendung bei Thuswaldner und Tichy [20], die ein Erdős-Kac Theorem für Systeme q-additiver Funktionen bewiesen. Das ursprüngliche Erdős-Kac Theorem kann in [9] nachgelesen werden.

Es wurde die Vermutung aufgestellt, dass die Exponenten in der Primfaktorzerlegung von $n!$ ebenfalls auf den Restklassen modulo eines Tupels aus positiven ganzen Zahlen $\mathbf{m}$ gleichverteilt sind. Im Folgenden wird beschrieben, wie sich diese Vermutung entwickelte. Ziel dieser Arbeit ist es, die Vermutung für den Fall zu beweisen, dass das Tupel $\mathbf{m}$ aus Primzahlen bzw. Primzahlpotenzen oder aus Zahlen, die von der jeweiligen Primzahl nicht geteilt werden, besteht.

Für eine Primzahl p und eine positive ganze Zahl n sei $e_p(n!)$ der Exponent, mit dem p in der Primfaktorzerlegung von $n!$ auftritt. In [8] fragten Erdős und Graham, ob zu jeder festen positiven ganzen Zahl k eine positive ganze Zahl n existiert, so dass die ersten k Exponenten in der Primfaktorzerlegung von $n!$, also $e_{p_1}(n!), \ldots, e_{p_k}(n!)$,

gerade sind, wobei $p_1 < p_2 < \cdots < p_k$ die ersten k Primzahlen seien. Diese Frage wurde von Berend [1] positiv beantwortet. Er zeigte, dass für ein k unendlich viele positive ganze Zahlen $1 = n_0 < n_1 < n_2 < \cdots$ existieren, so dass für jedes j die Zahlen $e_{p_1}(n_j!), e_{p_2}(n_j!), \ldots, e_{p_k}(n_j!)$ gerade sind und dass $n_{j+1} - n_j \leq C \quad (j = 1, 2, \ldots)$ gilt, wobei C nur von k abhängt und eine berechenbare Konstante ist. Dieses Ergebnis wurde von Chen und Zhu in [5] wie folgt erweitert. Falls für $\varepsilon_i \in \{0, 1\}$ $(1 \leq i \leq k)$ mindestens ein n existiert, so dass $e_{p_i}(n!) \equiv \varepsilon_i \bmod 2$ für alle $i = 1, \ldots, k$ gilt, so existieren unendlich viele positive ganze Zahlen n mit dieser Eigenschaft und der Abstand zweier aufeinander folgender Zahlen dieser Art ist durch eine Konstante beschränkt, die wiederum nur von k abhängt. Außerdem bewies Chen [4] die Vermutung von Erdős und Graham für einen allgemeineren Fall. Im Detail zeigte er, dass für eine gegebene positive ganze Zahl k und $\varepsilon_i \in \{0, 1\}$ $(1 \leq i \leq k)$ unendlich viele positive ganze Zahlen n mit

$$e_{p_i}(n!) \equiv \varepsilon_i \bmod 2 \qquad (1 \leq i \leq k)$$

existieren. Sander [18] stellte diesbezüglich eine stärkere Vermutung auf und zwar dass gilt

$$|\{1 \leq n < N : e_{p_i}(n!) \equiv \varepsilon_i \bmod 2 \ (1 \leq i \leq k)\}| \sim \frac{N}{2^k} \quad \text{für } N \to \infty,$$

wobei es sich bei den Primzahlen $p_1, \ldots, p_k$ um k verschiedene Primzahlen handelt, die aber nicht zwingend die ersten k sein müssen. Luca und Stănică [16] verallgemeinerten diese Vermutung wie folgt. Seien $p_1, \ldots, p_k$ verschiedene Primzahlen, $m_1, \ldots, m_k \geq 2$ beliebige positive ganze Zahlen und $0 \leq a_i \leq m_i - 1$ beliebige Restklassen modulo m_i. Dann wird vermutet, dass

$$|\{1 \leq n < N : e_{p_i}(n!) \equiv a_i \bmod m_i \ (1 \leq i \leq k)\}| \sim \frac{N}{m_1 \cdots m_k} \quad \text{für } N \to \infty$$

gilt. Sie bewiesen die Aussage

$$|\{1 \leq n < N : e_{p_i}(n!) \equiv a_i \bmod m_i \ (1 \leq i \leq k)\}| = \frac{N}{m_1 \cdots m_k} + \mathcal{O}\left(N^{1-\delta}\right),$$

für den Fall, dass $p_i \nmid m_i$ für $i = 1, \ldots, k$ gilt, indem sie eine vollständig q-additive Funktion definierten, die zum einen kongruent zu $e_{p_i}(n!)$ ist und zum anderen den Voraussetzungen entspricht, die von Kim in [14] formuliert wurden, und wendeten die Aussage von Kim an. Da aber bei der Konstruktion der Funktion der kleine Satz von Fermat mit eingeht, muss man für den Fall $p_i \mid m_i$ eine andere Funktion wählen. Luca und Stănică schlagen für den Fall $m_i = 2$ die Ziffernsumme vor, da für diese

$S_2(n) \equiv e_2(n!) - n_0$ gilt, wobei n_0 die 0-te Ziffer der dyadischen Entwicklung von n sei. Nimmt man an, dass $p_1 = 2$ ist, so sind dann die Kongruenzsysteme

$$f_i(2n) \equiv \varepsilon_i \bmod 2 \quad \text{für } i = 1, \ldots, k$$

und

$$f_1(2n+1) \equiv \varepsilon_1 + 1 \bmod 2, \quad f_i(2n+1) \equiv \varepsilon_i \bmod 2 \quad \text{für } i = 2, \ldots, k$$

zu betrachten, wobei f_1 die Ziffernsumme sei und f_i für $i = 2, \ldots, k$ wie in [16] definiert seien. Um nun aber mit Hilfe dieser Kongruenzen die gewünschte Aussage zu schließen, bedarf es einer Verallgemeinerung des Satzes von Kim, die besagt, dass die Zahlen $\mathbf{f}(\mathbf{u}n + \mathbf{v})$, wobei $\mathbf{f} = (f_1, \ldots, f_l)$, die f_i vollständig q_i-additive Funktionen mit ganzzahligen Werten und $\mathbf{u}$ und $\mathbf{v}$ l-Tupel aus ganzen Zahlen mit bestimmtem Eigenschaften seien, auf den Restklassen modulo $\mathbf{m}$ mit $\mathbf{m} = (m_1, \ldots, m_l)$ gleichverteilt sind.

1.2 Aufbau der Arbeit

Im zweiten Kapitel dieser Arbeit werden die vollständig q-additiven Funktionen zunächst näher charakterisiert. Insbesondere wird gezeigt, dass diese bereits durch die Angabe der ersten q Werte eindeutig festgelegt sind. Im zweiten Teil dieses Kapitels werden erste Grundlagen für einen späteren Beweis gelegt, indem die Weyl-van der Corput Ungleichung für die Abschätzung von Exponentialsummen verwendet wird.

In dem darauf folgenden Kapitel werden zunächst wesentliche Ergebnisse von Kim sowie die Voraussetzungen, die die betrachteten vollständig q-additiven Funktionen erfüllen müssen, dargestellt.

Im vierten Kapitel werden die Voraussetzungen für die vollständig q-additiven Funktionen für den allgemeineren Fall modifiziert und

$$|\{0 \le n < N : \mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}\}| = \frac{N}{m_1 m_2 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right)$$

bewiesen, wobei $0 < \delta < 1$ eine Konstante ist, die nur von $\mathbf{q}$, $\mathbf{m}$ und von der Länge dieser Tupel abhängt. Des weiteren werden Folgerungen betrachtet, die sich aus dieser Aussage ergeben.

Im fünften Kapitel wird zunächst das Vorgehen von Luca und Stănică behandelt, die in [16] eine vollständig q-additive Funktion konstruierten, auf die sich die Aussage von Kim anwenden lässt. Gemäß der Idee von Luca und Stănică wird daraufhin die Ziffernsumme sowie das Ergebnis aus dem vierten Kapitel verwendet, um den Fall $m_i = p_i^{\alpha_i}$ zu beweisen. Für den allgemeinen Fall $m_i = k_i p_i^{\alpha_i}$ mit $(k_i, p_i^{\alpha_i}) = 1$ wird ein Ergebnis von Berend und Kolesnik [2] angeführt. Diese konstruierten eine Funktion, die kongruent modulo k_i bzw. modulo $p_i^{\alpha_i}$ ist, um dann hierauf eine von ihnen gezeigte Variante des Satzes von Kim anzuwenden. Für den Fall $\alpha_i = 1$, geht aus dem Beweis nicht genau hervor, wie die Aussage folgt, weshalb dieser Fall hier ausgeschlossen wird. Abschließend wird die Güte des Fehlerterms betrachtet.

1.3 Danksagung

An dieser Stelle möchte ich besonders Herrn Prof. Dr. Sander für die sehr gute Betreuung dieser Arbeit sowie für die stetige Unterstützung danken. Herrn Prof. Dr. Elsner danke ich für die freundliche Bereitschaft, das Korreferat dieser Dissertation zu übernehmen.

Auch Herrn Dr. Luca möchte ich ganz herzlich für den Hinweis auf einen Artikel von D. Berend und G. Kolesnik danken.

Darüber hinaus danke ich all meine Freunden sowie meinen Eltern für die langjährige Unterstützung.

Kapitel 2

Grundlagen

In diesem Kapitel werden zunächst die vollständig q-additiven Funktionen betrachtet und näher charakterisiert. Insbesondere wird gezeigt, dass sie einen $\mathbb{C}$-Vektorraum bilden. Eine Basis dieses Vektorraums wird angegeben. Außerdem wird erläutert, warum die vollständig q-additiven Funktionen bereits durch die Angabe der ersten q Werte eindeutig festgelegt sind.

Im zweiten Abschnitt des Kapitels wird eine Abschätzung von Exponentialsummen erläutert, die mit Hilfe der Weyl-van der Corput Ungleichung vorgenommen wird. Diese Abschätzung wird in Lemma 2.4 explizit formuliert und findet im vierten Kapitel Anwendung in Proposition 4.9.

2.1 Vollständig q-additive Funktionen

Man beachte, dass nicht jede q-additive Funktion auch vollständig q-additiv ist, auch wenn die beiden Begriffe in der Literatur nicht immer deutlich voneinander unterschieden werden. Ein Beispiel einer q-additiven Funktion, die keine vollständig q-additive Funktion ist, ist die van der Corput Folge $x(n)$ (siehe hierzu [15]). Diese ist 2-additiv und definiert durch $x(n) = \sum_{j=0}^{s} a_j 2^{-j-1}$, wobei $n = \sum_{j=0}^{s} a_j 2^j$ die dyadische Entwicklung von n sei.

Sei nun V_q definiert durch $V_q = \{f : \mathbb{N} \cup \{0\} \to \mathbb{C} : f \text{ ist vollständig } q\text{-additiv}\}$. Es

seien $f, g \in V_q$, a, b, k ganze Zahlen mit $a, k \geq 1$, $0 \leq b < q$ und c eine komplexe Zahl. Dann gilt

$$(f+g)(0) = f(0) + g(0) = 0,$$

$$\begin{aligned}(f+g)(aq^k+b) &= f(aq^k+b) + g(aq^k+b) \\ &= f(a) + f(b) + g(a) + g(b) \\ &= (f+g)(a) + (f+g)(b)\end{aligned}$$

und

$$\begin{aligned}(cf)(aq^k+b) &= cf(aq^k+b) \\ &= c\,(f(a) + f(b)) \\ &= (cf)(a) + (cf)(b).\end{aligned}$$

Somit ist V_q ein $\mathbb{C}$-Vektorraum.

Offenbar ist eine vollständig q-additive Funktion $f \in V_q$ durch die ersten q Werte, also $f(0), f(1), f(2), \ldots, f(q-1)$, eindeutig festgelegt, denn zum einen lässt sich jede nicht negative ganze Zahl eindeutig schreiben als $aq^k + b$ mit $0 \leq a < q$, $0 \leq b < q^k$ und $k \in \mathbb{N}$. Zum anderen ist durch die Vorgabe der ersten q Werte auch

$$f(aq+b) = f(a) + f(b) \quad (0 \leq a, b < q)$$

eindeutig bestimmt. Hieraus ergeben sich wiederum eindeutig die Werte für

$$f(aq^2+b) = f(a) + f(b) \quad (0 \leq a < q, 0 \leq b < q^2).$$

Dieses Argument lässt sich fortsetzen.

Daher bilden die Funktionen e_i $(1 \leq i \leq q-1)$ mit

$$e_i(x) = \begin{cases} 1 & \text{für } x = i, \\ 0 & \text{für } 1 \leq x < q, x \neq i, \end{cases}$$

die für $x \geq q$ vollständig q-additiv fortgesetzt werden, eine Basis von V_q.

Satz 2.1 *Sei x eine positive ganze Zahl und e_i sei wie zuvor definiert. Dann ist $e_i(x)$ gleich der Anzahl der Ziffern in der q-adischen Entwicklung von x, die gleich i sind.*

Beweis. Für die Zahlen $1, 2, \ldots, q-1$ besteht die q-adische Entwicklung nur aus einer Ziffer und dies ist die Zahl selbst. Also gilt der Satz für diese Zahlen laut Definition der Funktionen e_i. Sei nun die Aussage für alle natürlichen Zahlen kleiner $n \in \mathbb{N}$ mit $q|n$ erfüllt. Es gilt

$$e_i(n) = e_i\left(\frac{n}{q}q\right) = e_i\left(\frac{n}{q}\right) \quad (1 \leq i \leq q-1),$$

da e_i vollständig q-additiv ist. Nach Voraussetzung ist dies die Häufigkeit, mit der die Ziffer i in der q-adischen Entwicklung von $\frac{n}{q}$ auftritt. Da q das n teilt, ist die 0-te Ziffer n_0 der q-adischen Entwicklung von n gleich Null. Damit unterscheiden sich die q-adischen Entwicklungen von n und $\frac{n}{q}$ nur in den Exponenten von q. Somit sind auch die Anzahlen der Ziffern gleich und die Aussage folgt für n.

Da eine vollständig q-additive Funktion insbesondere q-additiv ist, gilt

$$e_i(n+k) = e_i\left(\frac{n}{q}q + k\right) = e_i\left(\frac{n}{q}q\right) + e_i(k) = e_i(n) + e_i(k) \quad (1 \leq i, k \leq q-1).$$

Für n ist die Aussage bereits gezeigt. Zum einen ist laut Definition $e_i(k) = 1$ im Fall $i = k$, zum anderen unterscheiden sich n und $n+k$ in ihrer q-adischen Entwicklung nur in der 0-ten Ziffer. Es gilt $n_0 = 0$ und $(n+k)_0 = k$ und es folgt der Satz. □

Bemerkung 2.2 Durch diesen Satz lässt sich die Ziffernsumme S_q darstellen als

$$S_q(n) = \sum_{i=1}^{q-1} i e_i(n).$$

Hieraus folgt direkt, dass man die Ziffernsumme nur insofern modifizieren kann, dass man sie mit $c \in \mathbb{C}$ multipliziert und sie trotzdem vollständig q-additiv bleibt. Gewichtet man die einzelnen Ziffern unterschiedlich, addiert man zum Beispiel nur jede zweite Ziffer, so ist die modifizierte Ziffernsumme nicht mehr vollständig q-additiv.

2.2 Die Weyl-van der Corput Ungleichung

Eine Exponentialsumme ist eine Summe der Form

$$\sum_{a<n\leq b} e\left(f(n)\right),$$

wobei $f(n)$ eine reellwertige Funktion ist und die Funktion e durch $e(x) = e^{2\pi ix}$ definiert sei. Im folgenden werden Summen der Form

$$S = \sum_{n \in I} e\left(f(n)\right) \tag{2.1}$$

abgeschätzt, wobei $I = (a, b]$ und a, b ganze Zahlen seien. Durch die Dreiecksungleichung ergibt sich die folgende triviale Abschätzung

$$|S| \leq \sum_{n \in I} |e\left(f(n)\right)| = |I| = b - a,$$

wobei ausgenutzt wird, dass es sich bei den komplexen Zahlen $e\left(f(n)\right)$ um Punkte auf dem Einheitskreis handelt, die somit dem Betrage nach 1 sind. Nun wird es sicherlich nur im Spezialfall gegeben sein, dass die triviale Abschätzung bestmöglich ist. So werden sich zum Beispiel zwei Punkte, die sich gegenüber liegen, gegenseitig auslöschen. Es ist wünschenswert, eine genauere Abschätzung zu finden. Hierbei ist die nun folgende Weyl-van der Corput Ungleichung behilflich, deren Beweis in [12] nachzulesen ist.

Lemma 2.3 [12, Lemma 2.5] *Seien $I = (a, b]$ mit ganzen Zahlen a und b und $\xi(n)$ eine komplexwertige Funktion mit der Eigenschaft $\xi(n) = 0$, falls $n \notin I$ ist. Für eine positive ganze Zahl H gilt*

$$\left|\sum_n \xi(n)\right|^2 \leq \frac{|I| + H}{H} \sum_{|h|<H} \left(1 - \frac{|h|}{H}\right) \sum_n \xi(n)\overline{\xi(n-h)}.$$

Die folgenden Überlegungen sind ebenfalls [12] entnommen. Man definiere

$$\xi(n) = \begin{cases} e\left(f(n)\right) & \text{falls } n \in I \\ 0 & \text{sonst} \end{cases}$$

und es sei

$$S_1 = \sum_{n \in I(h)} e\left(f(n+h) - f(n)\right),$$

wobei $I(h) = \{n : n \in I \text{ und } n + h \in I\}$ und h eine ganze Zahl ist. Damit lässt sich (2.1) mit der Weyl-van der Corput Ungleichung wie folgt abschätzen

$$|S|^2 \leq \frac{|I| + H}{H} \sum_{|h|<H} |S_1(h)|.$$

Nimmt man nun noch an, dass $H \leq |I|$ ist und nutzt aus, dass $S_1(-h) = \overline{S_1(h)}$ gilt, so erhält man

$$|S|^2 \leq \frac{2\,|I|^2}{H} + \frac{4\,|I|}{H} \sum_{1 \leq h \leq H} |S_1(h)|\,. \tag{2.2}$$

Aus (2.2) erhält man direkt das folgende Lemma.

Lemma 2.4 *Seien $1 \leq K \leq N$ ganze Zahlen. Dann gilt*

$$\left| \sum_{n=0}^{N-1} e\,(f(n)) \right|^2 \leq \frac{2N^2}{K} + \frac{4N}{K} \sum_{k=1}^{K} \left| \sum_{n=0}^{N-k-1} e\,(f(n+k) - f(n)) \right|. \tag{2.3}$$

Dieses Lemma wird ein wichtiges Hilfsmittel sein, um die Exponentialsummen, die im vierten Kapitel und insbesondere in Proposition 4.9 verwendet werden, abzuschätzen.

Kapitel 3

Der Satz von Kim

In diesem Kapitel werden wichtige Ergebnisse von Kim [14] dargestellt. Zunächst wird definiert, wann ein l-Tupel $\mathbf{a}$ bezüglich der l-Tupel $\mathbf{q}$, $\mathbf{m}$ und $\mathbf{f}$ zulässig ist, wobei $\mathbf{q}$, $\mathbf{m}$ aus ganzen Zahlen ≥ 2 und $\mathbf{f}$ aus vollständig q_j-additiven Funktionen mit ganzzahligen Werten bestehen. Mit Hilfe dieser zulässigen l-Tupel wird der Satz von Kim, Satz 3.2, formuliert, der in Abhängigkeit der Anzahl der zulässigen Tupel $\mathbf{a}$ eine Abschätzung angibt, wie viele $0 \leq n < N$ mit $\mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}$ für feste $\mathbf{a}$ und $\mathbf{m}$ existieren, wobei die Kongruenzen komponentenweise zu betrachten sind. Die Hauptfolgerung hieraus stellt das Korollar 3.3 dar. Außerdem werden einige technische Hilfsmittel von Kim aufgeführt, die in Kapitel 4 weitere Verwendung finden.

Gegeben seien die l-Tupel $\mathbf{q} = (q_1, q_2, \ldots, q_l)$ und $\mathbf{m} = (m_1, m_2, \ldots, m_l)$ aus ganzen Zahlen mit $q_j, m_j \geq 2$ für $j = 1, \ldots, l$ und $(q_i, q_j) = 1$ für $i \neq j$. Für jedes j sei f_j eine vollständig q_j-additive Funktion mit ganzzahligen Werten und es sei $\mathbf{f} = (f_1, f_2, \ldots, f_l)$. Weiterhin definiere man

$$F_j = f_j(1), \tag{3.1}$$

$$d_j = \mathrm{ggT}\{m_j, (q_j - 1)F_j, f_j(r) - rF_j \ (2 \leq r \leq q_j - 1)\} \tag{3.2}$$

und es seien $\mathbf{F} = (F_1, F_2, \ldots, F_l)$, $\mathbf{d} = (d_1, d_2, \ldots, d_l)$. Abkürzend wird $\mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}$ geschrieben, wenn $f_j(n) \equiv a_j \mod m_j$ für jeden Index j gilt.

Definition 3.1 *Ein l-Tupel $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ aus ganzen Zahlen heißt* zulässig

bezüglich $\mathbf{q}$, $\mathbf{m}$ *und* $\mathbf{f}$, *wenn das Kongruenzsystem*

$$\mathbf{F}n \equiv \mathbf{a} \mod \mathbf{d}$$

eine Lösung n *besitzt.*

Mit der Notation

$$\mathcal{A} = \{\mathbf{a} = (a_1, a_2, \ldots, a_l) : 0 \leq a_j \leq m_j - 1 \ (1 \leq j \leq l), \ \mathbf{a} \text{ zulässig bzgl. } \mathbf{q}, \mathbf{m} \text{ und } \mathbf{f}\}$$

kann nun der Satz von Kim formuliert werden.

Satz 3.2 [14, Theorem] *Seien* $\mathbf{q}$, $\mathbf{m}$ *und* $\mathbf{f}$ *wie zuvor definiert. Für beliebige ganzzahlige* l*-Tupel* $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ *und alle positiven ganzen Zahlen* N *gilt*

$$\begin{aligned} &|\{0 \leq n < N : \mathbf{f}(n) \equiv \mathbf{a} \mod \mathbf{m}\}| \\ &\qquad = \begin{cases} \frac{N}{|\mathcal{A}|} + \mathcal{O}\left(N^{1-\delta}\right) & \textit{falls } \mathbf{a} \textit{ zulässig ist} \\ 0 & \textit{sonst,} \end{cases} \end{aligned} \tag{3.3}$$

wobei $\delta = \frac{1}{120 l^2 \overline{q}^3 \overline{m}^2}$ *ist, mit* $\overline{q} = \max_{1 \leq i \leq l} q_i$ *und* $\overline{m} = \max_{1 \leq i \leq l} m_i$ *und die Konstante des* $\mathcal{O}$*-Terms nur von* l *und* $\mathbf{q}$ *abhängt.*

Aus Satz 3.2 schließt Kim das folgende wichtige Korollar, welches Luca und Stănică [16] verwenden, um ihren Satz über die Verteilung der Exponenten in der Primfaktorzerlegung von $n!$ zu beweisen (siehe hierzu auch Kapitel 5, Satz 5.1).

Korollar 3.3 [14, Corollary 1] *Seien* $\mathbf{q}$, $\mathbf{m}$, $\mathbf{f}$ *und* δ *wie in Satz 3.2 gegeben. Dann gilt*

$$|\{0 \leq n < N : \mathbf{f}(n) \equiv \mathbf{a} \mod \mathbf{m}\}| = \frac{N}{m_1 m_2 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right)$$

für alle Tupel $\mathbf{a}$ *genau dann, wenn*

$$\begin{aligned} (F_j, d_j) &= 1 \qquad (1 \leq j \leq l), \\ (d_i, d_j) &= 1 \qquad (1 \leq i < j \leq l). \end{aligned}$$

Im folgenden ist eine Auswahl der Lemmata aufgeführt, die in [14] im Beweis von Satz 3.2 verwendet werden und die auch in der Verallgemeinerung im folgenden Kapitel benötigt werden. $e(x)$ bezeichne hier wie auch in der restlichen Arbeit $e^{2\pi ix}$.

Lemma 3.4 [14, Lemma 1] *Für positive ganze Zahlen n und m gilt*

$$\frac{1}{m}\sum_{k=0}^{m-1} e\left(\frac{n}{m}k\right) = \begin{cases} 1 & \text{falls } m|n, \\ 0 & \text{sonst.} \end{cases}$$

Lemma 3.5 [14, Lemma 3] *Seien $1 \leq K \leq N$ ganze Zahlen und seien a_n komplexe Zahlen mit $|a_n| \leq 1$ für $n = 0, 1, \ldots, N-1$. Dann gilt*

$$\left|\frac{1}{N}\sum_{n=0}^{N-1} a_n - \frac{1}{K}\sum_{n=0}^{K-1} a_n\right| \leq \frac{2(N-K)}{N}.$$

Lemma 3.6 [14, Lemma 7] *Seien $q \geq 2$ und $m \geq 2$ positive ganze Zahlen. Außerdem sei f eine vollständig q-additive Funktion. F und d seien wie F_j und d_j in (3.1) und (3.2) in Beziehung zu q und m durch*

$$F = f(1) \tag{3.4}$$

$$d = \mathrm{ggT}\{m_j, (q-1)F, f(r) - rF(2 \leq r \leq q-1)\} \tag{3.5}$$

definiert. Dann gilt für jede nicht negative ganze Zahl n die Kongruenz

$$f(n) \equiv nF \mod d. \tag{3.6}$$

Es sei nun h eine ganze Zahl, so dass $m \nmid dh$ gilt und es sei $g(n) = e\left(\frac{h}{m}f(n)\right)$, mit einer vollständig q-additiven reellwertigen Funktion f. Weiterhin seien zwei Korrelationsfunktionen definiert durch

$$\begin{aligned} \Phi_N(k) &= \frac{1}{N}\sum_{n=0}^{N-1} \overline{g(n)}g(n+k) \\ \Phi_{K,N}(r) &= \frac{1}{K}\sum_{k=0}^{K-1} \overline{\Phi_N(k)}\Phi_N(k+r). \end{aligned}$$

Lemma 3.7 [14, Lemma 9] *Für jede ganze Zahl k und $0 \leq r \leq q-1$ gilt*

$$\Phi_{qN}(qk+r) = \alpha_r \Phi_N(k) + \beta_r \Phi_N(k+1),$$

wobei

$$\begin{aligned} \alpha_r &= \frac{1}{q} \sum_{i=0}^{q-r-1} \overline{g(i)} g(i+r), \\ \beta_r &= \frac{1}{q} \sum_{i=q-r}^{q-1} \overline{g(i)} g(i+r-q) \quad (1 \leq r \leq q-1), \quad \beta_0 = 0. \end{aligned}$$

Für α_r und β_r gilt

$$|\alpha_r| \leq \frac{q-r}{q}, |\beta_r| \leq \frac{r}{q} \quad (1 \leq r \leq q-1).$$

Lemma 3.8 [14, Lemma 10] *Für $r = 0, 1$ gilt*

$$\Phi_{qK,qN}(r) = \lambda_r \Phi_{K,N}(0) + \mu_r \Phi_{K,N}(1) + \nu_r \overline{\Phi_{K,N}(1)} + E_{K,N}(r),$$

wobei

$$\begin{aligned} \lambda_r &= \frac{1}{q} \sum_{i=0}^{q-1} \left(\overline{\alpha_i} \alpha_{i+r} + \overline{\beta_i} \beta_{i+r} \right), \\ \mu_r &= \frac{1}{q} \sum_{i=0}^{q-1} \overline{\alpha_i} \beta_{i+r}, \\ \nu_r &= \frac{1}{q} \sum_{i=0}^{q-1} \overline{\beta_i} \alpha_{i+r}. \end{aligned}$$

Für den Restterm $E_{K,N}(r)$ gilt

$$|E_{K,N}(r)| \leq \frac{2}{K}.$$

α_i und β_i seien für $0 \leq i \leq q-1$ wie in Lemma 3.7 definiert und es seien $\alpha_q = 0$ und $\beta_q = 1$. Dann gilt die Ungleichung

$$|\lambda_r| + |\mu_r| + |\nu_r| \leq 1 \qquad \text{für } r \in \{0, 1\}.$$

Lemma 3.9 [14, Lemma 13] *Für $r = 0, 1$ und eine positive ganze Zahl i gilt*

$$\Phi_{q^{2i}K,q^{2i}N}(r) \leq e^{-\tau i} \left(1 + \frac{7q^2}{K}\right),$$

wobei $\tau = \frac{1}{q^2 m^2}$ ist.

Kapitel 4

Eine Verallgemeinerung des Satzes von Kim

In diesem Kapitel wird zunächst der Begriff der Zulässigkeit von $\mathbf{a}$ bezüglich $\mathbf{q}$, $\mathbf{m}$ und $\mathbf{f}$, der von Kim eingeführt wurde und sich auf Kongruenzen der Form $n\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}$ bezieht, auf Kongruenzen der Form $(\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}$ übertragen, was zu dem Begriff der Zulässigkeit bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$ führt. Daraufhin wird in Satz 4.2 eine Verallgemeinerung des Satzes von Kim formuliert. Dieser gibt in Abhängigkeit der Anzahl der zulässigen Tupel $\mathbf{a}$ bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$ eine Abschätzung an, wie viele $0 \leq n < N$ mit $\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}$ für feste $\mathbf{a}$, $\mathbf{m}$, $\mathbf{u}$ und $\mathbf{v}$ existieren, wobei die Kongruenzen wiederum komponentenweise zu betrachten sind. Satz 4.2 stellt ein wesentliches Resultat dieser Arbeit dar.

Im zweiten Abschnitt des Kapitels werden die Voraussetzungen für den Beweis von Satz 4.2 geschaffen. Insbesondere wird Proposition 4.9 hergeleitet, welche im Beweis des Satzes den Fehlerterm liefern wird. Außerdem werden in Lemma 4.11 die Tupel $\mathbf{a}$, die zulässig bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$ sind, näher charakterisiert.

Daraufhin wird im dritten Abschnitt des Kapitel schließlich der eigentliche Beweis der Verallgemeinerung des Satzes von Kim, Satz 4.2, durchgeführt.

Im vierten Abschnitt werden einige Folgerungen aus Satz 4.2 bewiesen, wobei Korollar 4.12 die wichtigste Folgerung darstellt. Diese wird im fünften Kapitel dazu dienen, die Gleichverteilung der Exponenten in der Primfaktorzerlegung von $n!$ auf den

Restklassen modulo $\mathbf{m}$ zu beweisen, wobei die Einträge des Tupels $\mathbf{m}$ Primzahlen bzw. Primzahlpotenzen sind oder diese zu den Primzahlen der betrachteten Exponenten teilerfremd sind. Korollar 4.12 gibt eine Abschätzung der Anzahl der $0 \leq n < N$ mit $\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}$ in Abhängigkeit des Tupels $\mathbf{m}$ an, wobei die Tupel $\mathbf{q}$, $\mathbf{u}$ und $\mathbf{f}$ bestimmte Voraussetzungen zu erfüllen haben. Satz 4.13 stellt einen Spezialfall des Satzes 4.2 dar, wobei lediglich die Länge der verwendeten Tupel verdoppelt ist und die Einträge innerhalb der Tupel $\mathbf{u}$ und $\mathbf{v}$ jeweils gleich sind, also $\mathbf{u} = (u, u, \ldots, u)$ und $\mathbf{v} = (v, v, \ldots, v)$ für geeignete ganze Zahlen u und v gilt. Korollar 4.14 ist die entsprechende Folgerung aus diesem Satz. Es dient an dieser Stelle dazu, die Hauptresultate dieses Kapitels mit einem Satz von Berend und Kolesnik, der als Satz 4.15 zitiert wird, in Beziehung zu setzen. Dies wird in Bemerkung 4.16 genauer erläutert. Berend und Kolesnik arbeiteten parallel zu der Entstehung dieser Arbeit an der gleichen Fragestellung.

Eine Abbildung am Ende dieses Kapitels gibt eine Übersicht über die Beweiskette, die bis zum Beweis von Satz 4.2 und Korollar 4.12 aufgebaut wird. Im mittleren Bereich der Abbildung sind die Resultate – bis zum entscheidenden Korollar – aufgeführt, die in der Arbeit selbst bewiesen werden, und dies in der Reihenfolge in der sie bewiesen werden. Die Lemmata rechts und links, welche etwas dunkler hinterlegt sind, sind Resultate anderer Autoren. Die Pfeile besagen, welche Aussagen für den Beweis der anderen benötigt werden.

4.1 Die Verallgemeinerung des Satzes

Gegeben seien wie auch schon im Kapitel zuvor die l-Tupel $\mathbf{q} = (q_1, q_2, \ldots, q_l)$ und $\mathbf{m} = (m_1, m_2, \ldots, m_l)$ mit $q_j, m_j \geq 2$ für $j = 1, \ldots, l$ und $(q_i, q_j) = 1$ für $i \neq j$. Für jedes j sei f_j eine vollständig q_j-additive Funktion mit ganzzahligen Werten, es sei $\mathbf{f} = (f_1, f_2, \ldots, f_l)$. Man definiere

$$F_j = f_j(1), \tag{4.1}$$

$$d_j = \mathrm{ggT}\{m_j, (q_j - 1)F_j, f_j(r) - rF_j(2 \leq r \leq q_j - 1)\} \tag{4.2}$$

und es seien $\mathbf{F} = (F_1, F_2, \ldots, F_l)$, $\mathbf{d} = (d_1, d_2, \ldots, d_l)$. Zusätzlich seien zwei weitere l-Tupel $\mathbf{u} = (u_1, u_2, \ldots, u_l)$ und $\mathbf{v} = (v_1, v_2, \ldots, v_l)$ gegeben, für die $u_j \geq 1$ und

$v_j \geq 0$ für $j = 1, \ldots, l$ sowie $\left(u_j, q_j^{t_j}\right) = (u_j, q_j)$ für $t_j \geq 2$ gilt. Abkürzend wird $\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}$ geschrieben, wenn $f_j(u_j n + v_j) \equiv a_j \bmod m_j$ für jeden Index j gilt. Man definiere außerdem $\overline{u} = \max_{1 \leq i \leq l} u_i$.

Definition 4.1 *Ein l-Tupel $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ aus ganzen Zahlen heißt* zulässig *bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$, wenn das Kongruenzsystem*

$$(\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \mod \mathbf{d}$$

eine Lösung n besitzt.

Mit der Notation

$$\mathcal{A} = \big\{\mathbf{a} = (a_1, a_2, \ldots, a_l) : 0 \leq a_j \leq m_j - 1 \ (1 \leq j \leq l), \\ \mathbf{a} \text{ zulässig bzgl. } \mathbf{q}, \mathbf{m}, \mathbf{u}, \mathbf{v} \text{ und } \mathbf{f}\big\}$$

wird nun die Verallgemeinerung des Satzes von Kim formuliert.

Satz 4.2 *Seien $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$ wie zuvor definiert. Für beliebige ganzzahlige l-Tupel $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ und alle positiven ganzen Zahlen N gilt*

$$|\{0 \leq n < N : \mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}\}| \\ = \begin{cases} \frac{N}{|\mathcal{A}|} + \mathcal{O}\left(N^{1-\delta}\right) & \textit{falls } \mathbf{a} \textit{ zulässig ist} \\ 0 & \textit{sonst,} \end{cases} \tag{4.3}$$

wobei $\delta = \frac{1}{120 l^2 \overline{q}^3 \overline{m}^2}$ ist, mit $\overline{q} = \max_{1 \leq i \leq l} q_i$ und $\overline{m} = \max_{1 \leq i \leq l} m_i$ und die Konstante des $\mathcal{O}$-Terms nur von $\mathbf{q}$, $\mathbf{u}$ und l abhängt.

Der Beweis dieses Satzes wird in Abschnitt 4.3 erbracht.

4.2 Technische Hilfsmittel

Um die in Satz 4.2 formulierte Verallgemeinerung beweisen zu können, müssen zunächst einige Voraussetzungen geschaffen werden.

Lemma 4.3 *Sei f eine vollständig q-additive Funktion. Es seien t und i positive ganze Zahlen, $u \geq 1$ und $v \geq 0$ ebenfalls ganze Zahlen. Es sei $n \equiv r \bmod q^t$ $(0 \leq r < q^t)$ und $ur + v \equiv s \bmod q^t$ $(0 \leq s < q^t - i)$. Dann gilt*

$$f(un + v + i) - f(un + v) = f(s + i) - f(s).$$

Beweis. Aufgrund der obigen Kongruenzen existieren $b, m \in \mathbb{Z}$, so dass $n = bq^t + r$ und $ur + v = mq^t + s$ gilt. Nutzt man aus, dass f vollständig q-additiv ist, so kann man die folgende Rechnung aufstellen.

$$\begin{aligned}
f(un + v + i) - f(un + v) &= f(u(bq^t + r) + v + i) - f(u(bq^t + r) + v) \\
&= f(ubq^t + ur + v + i) - f(ubq^t + ur + v) \\
&= f(ubq^t + mq^t + s + i) - f(ubq^t + mq^t + s) \\
&= f((ub + m)q^t + s + i) - f((ub + m)q^t + s) \\
&= f(ub + m) + f(s + i) - f(ub + m) - f(s) \\
&= f(s + i) - f(s)
\end{aligned}$$

□

Proposition 4.4 *Seien N, K positive ganze Zahlen mit $\sqrt{N} \leq K \leq N$, q, m ebenfalls positive ganze Zahlen, f sei eine vollständig q-additive Funktion mit ganzzahligen Werten und d sei wie zuvor in (3.5) definiert. Darüber hinaus seien u, v ganze Zahlen mit $u \geq 1$ und $v \geq 0$ gegeben. Setze $U = (u, q)$. Dann gilt für eine beliebige ganze Zahl h mit $m \nmid dh$*

$$\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{N} \sum_{\substack{n=0 \\ n \equiv v \bmod U}}^{N-1} e\left(\frac{h}{m} \left(f(n + k) - f(n) \right) \right) \right|^2 = \mathcal{O}(N^{-\eta}), \tag{4.4}$$

wobei $\eta = \frac{1}{10q^3m^2}$ und die Konstante des $\mathcal{O}$-Terms nur von q abhängt.

Für den Beweis dieser Proposition werden einige weitere Lemmata benötigt, die im folgenden bewiesen werden. Wie schon zuvor sei h eine ganze Zahl, so dass $m \nmid dh$ und es sei $g(n) = e\left(\frac{h}{m} f(n)\right)$, wobei f eine vollständig q-additive reellwertige Funktion sei und $e(x)$ die Funktion $e^{2\pi i x}$ bezeichne. Für den Beweis der Proposition werden

zunächst die folgenden vier Korrelationsfunktionen definiert, wobei die ersten beiden bereits aus dem vorigen Kapitel bekannt sind.

$$\begin{aligned}
\Phi_N(k) &= \frac{1}{N}\sum_{n=0}^{N-1}\overline{g(n)}g(n+k)\\
\Phi_{K,N}(r) &= \frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k+r)\\
\Phi_N^*(k) &= \frac{1}{N}\sum_{\substack{n=0\\ n\equiv v \bmod U}}^{N-1}\overline{g(n)}g(n+k)\\
\Phi_{K,N}^*(r) &= \frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_N^*(k)}\Phi_N^*(k+r).
\end{aligned} \tag{4.5}$$

Damit ist die Behauptung (4.4) äquivalent zu

$$\Phi_{K,N}^*(0) = \mathcal{O}\left(N^{-\eta}\right). \tag{4.6}$$

Der Beweis dieser Aussage wird ab Seite 36 erbracht.

Lemma 4.5 *Für beliebige ganze Zahlen k und r mit $k \geq 0$ und $0 \leq r \leq q-1$ gilt*

$$\Phi_{qN}^*(qk+r) = a_r\Phi_N(k) + b_r\Phi_N(k+1) \tag{4.7}$$

mit

$$\begin{aligned}
a_r &= \frac{1}{q}\sum_{\substack{i=0\\ i\equiv v \bmod U}}^{q-r-1}\overline{g(i)}g(i+r)\\
b_r &= \frac{1}{q}\sum_{\substack{i=q-r\\ i\equiv v \bmod U}}^{q-1}\overline{g(i)}g(i+r-q), \quad (1\leq r\leq q-1), \quad b_0 = 0,
\end{aligned}$$

wobei

$$|a_r| \leq \frac{q-r}{q}, \quad |b_r| \leq \frac{r}{q} \quad (1\leq r\leq q-1). \tag{4.8}$$

Beweis. Es gilt

$$\begin{aligned}
g(aq+b) &= e\left(\frac{h}{m}f(aq+b)\right) = e\left(\frac{h}{m}\left(f(a)+f(b)\right)\right)\\
&= e\left(\frac{h}{m}f(a)\right)e\left(\frac{h}{m}f(b)\right) = g(a)g(b)
\end{aligned}$$

für $a \geq 0$ und $0 \leq b \leq q-1$. Hieraus ergibt sich, dass die Funktion g vollständig q-multiplikative ist. Vollständige q-multiplikative Funktionen werden entsprechend der vorigen Gleichung analog zu vollständige q-additiven Funktionen definiert. Diese Funktionen wurden unter anderem von Grabner [11] näher untersucht. Da laut Definition $U = (u, q)$ ist, gilt $U|q$ und man erhält mit Hilfe der vollständigen q-Multiplikativität von g

$$\begin{aligned}
qN\Phi^*_{qN}(qk+r) &= qN\frac{1}{qN}\sum_{\substack{n=0\\ n\equiv v \bmod U}}^{qN-1} \overline{g(n)}g(n+qk+r)\\
&= \sum_{\substack{n=0\\ n\equiv v \bmod U}}^{qN-1} \overline{g(n)}g(n+qk+r)\\
&= \sum_{i=0}^{q-1} \sum_{\substack{n=0\\ qn+i\equiv v \bmod U}}^{N-1} \overline{g(qn+i)}g(qn+i+qk+r)\\
&= \sum_{\substack{i=0\\ i\equiv v \bmod U}}^{q-r-1} \sum_{n=0}^{N-1} \overline{g(n)g(i)}g(n+k)g(i+r)\\
&\quad + \sum_{\substack{i=q-r\\ i\equiv v \bmod U}}^{q-1} \sum_{n=0}^{N-1} \overline{g(n)g(i)}g(n+k+1)g(i+r-q)\\
&= \sum_{\substack{i=0\\ i\equiv v \bmod U}}^{q-r-1} \overline{g(i)}g(i+r) \sum_{n=0}^{N-1} \overline{g(n)}g(n+k)\\
&\quad + \sum_{\substack{i=q-r\\ i\equiv v \bmod U}}^{q-1} \overline{g(i)}g(i+r-q) \sum_{n=0}^{N-1} \overline{g(n)}g(n+k+1)\\
&= (qN)a_r\Phi_N(k) + (qN)b_r\Phi_N(k+1).
\end{aligned}$$

Die Ungleichungen aus (4.8) folgen direkt, da die Werte der komplexwertigen Funktion g auf dem Rand des Einheitskreises liegen und somit dem Betrag nach gleich 1 sind und die Anzahl der Summanden $q-r$ bzw. r nicht überschreitet. □

Lemma 4.6 *Für $r = 0, 1$ gilt*

$$\Phi^*_{qK,qN}(r) = l_r\Phi_{K,N}(0) + m_r\Phi_{K,N}(1) + n_r\overline{\Phi_{K,N}(1)} + \varepsilon_{K,N}(r), \tag{4.9}$$

mit

$$\begin{aligned} |\varepsilon_{K,N}(r)| &\leq \frac{2}{K}, \\ l_r &= \frac{1}{q}\sum_{i=0}^{q-1}\left(\overline{a_i}a_{i+r} + \overline{b_i}b_{i+r}\right), \\ m_r &= \frac{1}{q}\sum_{i=0}^{q-1}\overline{a_i}b_{i+r}, \\ n_r &= \frac{1}{q}\sum_{i=0}^{q-1}\overline{b_i}a_{i+r}. \end{aligned}$$

a_i und b_i seien für $0 \leq i \leq q-1$ wie in Lemma 4.5 definiert und es seien $a_q = 0$ und $b_q = 1$. Dann gilt

$$|l_r| + |m_r| + |n_r| \leq 1 \qquad \text{für } r \in \{0,1\}. \tag{4.10}$$

Beweis. Laut Definition der Korrelationsfunktionen $\Phi^*_{K,N}$, Φ^*_K und Φ_N in (4.5) und mit Lemma 4.5 gilt

$$\begin{aligned} &qK\Phi^*_{qK,qN}(r) \\ &\quad = qK\frac{1}{qK}\sum_{k=0}^{qK-1}\overline{\Phi^*_{qN}(k)}\Phi^*_{qN}(k+r) \\ &\quad = \sum_{i=0}^{q-1}\sum_{k=0}^{K-1}\overline{\Phi^*_{qN}(qk+i)}\Phi^*_{qN}(qk+i+r) \\ &\quad = \sum_{i=0}^{q-r-1}\sum_{k=0}^{K-1}\left(\overline{a_i\Phi_N(k) + b_i\Phi_N(k+1)}\right)\left(a_{i+r}\Phi_N(k) + b_{i+r}\Phi_N(k+1)\right) \\ &\qquad + \sum_{i=q-r}^{q-1}\sum_{k=0}^{K-1}\left(\overline{a_i\Phi_N(k) + b_i\Phi_N(k+1)}\right)\left(a_{i+r}\Phi_N(k+1) + b_{i+r}\Phi_N(k+2)\right). \end{aligned}$$

Für $r = 0$ gilt also

$$qK\Phi^*_{qK,qN}(0) = \sum_{i=0}^{q-1}\sum_{k=0}^{K-1}\left(\overline{a_i\Phi_N(k) + b_i\Phi_N(k+1)}\right)\left(a_i\Phi_N(k) + b_i\Phi_N(k+1)\right)$$

$$
\begin{aligned}
&= \sum_{i=0}^{q-1} \sum_{k=0}^{K-1} \Big(\overline{a_i} a_i \overline{\Phi_N(k)} \Phi_N(k) + \overline{a_i} b_i \overline{\Phi_N(k)} \Phi_N(k+1) \\
&\qquad + \overline{b_i} a_i \overline{\Phi_N(k+1)} \Phi_N(k) + \overline{b_i} b_i \overline{\Phi_N(k+1)} \Phi_N(k+1) \Big) \\
&= \sum_{i=0}^{q-1} \Bigg(\sum_{k=0}^{K-1} \Big(\overline{a_i} a_i \overline{\Phi_N(k)} \Phi_N(k) + \overline{a_i} b_i \overline{\Phi_N(k)} \Phi_N(k+1) \\
&\qquad + \overline{b_i} a_i \overline{\Phi_N(k+1)} \Phi_N(k) + \overline{b_i} b_i \overline{\Phi_N(k)} \Phi_N(k) \Big) \\
&\qquad + \overline{b_i} b_i \overline{\Phi_N(K)} \Phi_N(K) - \overline{b_i} b_i \overline{\Phi_N(0)} \Phi_N(0) \Bigg) \\
&= \sum_{i=0}^{q-1} \left(\overline{a_i} a_i + \overline{b_i} b_i \right) \sum_{k=0}^{K-1} \overline{\Phi_N(k)} \Phi_N(k) \\
&\quad + \sum_{i=0}^{q-1} \overline{b_i} b_i \left(\overline{\Phi_N(K)} \Phi_N(K) - \overline{\Phi_N(0)} \Phi_N(0) \right) \\
&\quad + \sum_{i=0}^{q-1} \overline{a_i} b_i \sum_{k=0}^{K-1} \overline{\Phi_N(k)} \Phi_N(k+1) + \sum_{i=0}^{q-1} \overline{b_i} a_i \sum_{k=0}^{K-1} \overline{\Phi_N(k+1)} \Phi_N(k) \\
&= qK \left(l_0 \Phi_{K,N}(0) + m_0 \Phi_{K,N}(1) + n_0 \overline{\Phi_{K,N}(1)} + \varepsilon_{K,N}(0) \right)
\end{aligned}
$$

mit

$$
\varepsilon_{K,N}(0) = \frac{1}{qK} \sum_{i=0}^{q-1} \overline{b_i} b_i \left(\overline{\Phi_N(K)} \Phi_N(K) - \overline{\Phi_N(0)} \Phi_N(0) \right).
$$

Da $\Phi_N(0)$, $\Phi_N(K)$ und b_i dem Betrag nach höchstens 1 sind, gilt $|\varepsilon_{K,N}(0)| \leq \frac{2}{K}$.

Man betrachte nun den Fall $r = 1$. Da laut Definition $b_0 = 0$, $a_0 = b_q$ und $a_q = 0$ sind, gilt

$$
\begin{aligned}
&qK \Phi^*_{qK,qN}(1) \\
&\quad = \sum_{i=0}^{q-2} \sum_{k=0}^{K-1} \left(\overline{a_i \Phi_N(k) + b_i \Phi_N(k+1)} \right) \left(a_{i+1} \Phi_N(k) + b_{i+1} \Phi_N(k+1) \right) \\
&\qquad + \sum_{k=0}^{K-1} \left(\overline{a_{q-1} \Phi_N(k) + b_{q-1} \Phi_N(k+1)} \right) \left(a_0 \Phi_N(k+1) + b_0 \Phi_N(k+2) \right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=0}^{q-2}\sum_{k=0}^{K-1}\Big(\overline{a_i}a_{i+1}\overline{\Phi_N(k)}\Phi_N(k) + \overline{a_i}b_{i+1}\overline{\Phi_N(k)}\Phi_N(k+1) \\
&\quad + \overline{b_i}a_{i+1}\overline{\Phi_N(k+1)}\Phi_N(k) + \overline{b_i}b_{i+1}\overline{\Phi_N(k+1)}\Phi_N(k+1)\Big) \\
&\quad + \sum_{k=0}^{K-1}\Big(\overline{a_{q-1}}a_0\overline{\Phi_N(k)}\Phi_N(k+1) + \overline{b_{q-1}}a_0\overline{\Phi_N(k+1)}\Phi_N(k+1)\Big) \\
&= \sum_{i=0}^{q-2}\overline{a_i}a_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k) + \sum_{i=0}^{q-2}\overline{a_i}b_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k+1) \\
&\quad + \sum_{i=0}^{q-2}\overline{b_i}a_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k) + \sum_{i=0}^{q-2}\overline{b_i}b_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k+1) \\
&\quad + \overline{a_{q-1}}b_q\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k+1) + \overline{b_{q-1}}b_q\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k+1) \\
&= \sum_{i=0}^{q-1}\overline{a_i}a_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(q) + \sum_{i=0}^{q-1}\overline{a_i}b_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k+1) \\
&\quad + \sum_{i=0}^{q-1}\overline{b_i}a_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k) + \sum_{i=0}^{q-1}\overline{b_i}b_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k+1) \\
&= \sum_{i=0}^{q-1}\left(\overline{a_i}a_{i+1} + \overline{b_i}b_{i+1}\right)\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k) \\
&\quad + \sum_{i=0}^{q-1}\overline{b_i}b_{i+1}\Big(\overline{\Phi_N(K)}\Phi_N(K) - \overline{\Phi_N(0)}\Phi_N(0)\Big) \\
&\quad + \sum_{i=0}^{q-1}\overline{a_i}b_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\Phi_N(k+1)\sum_{i=0}^{q-1}\overline{b_i}a_{i+1}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\Phi_N(k) \\
&= qK\Big(l_1\Phi_{K,N}(0) + m_1\Phi_{K,N}(1) + n_1\overline{\Phi_{K,N}(1)} + \varepsilon_{K,N}(1)\Big),
\end{aligned}
$$

wobei

$$\varepsilon_{K,N}(1) = \frac{1}{qK}\sum_{i=0}^{q-1}\overline{b_i}b_{i+1}\Big(\overline{\Phi_N(K)}\Phi_N(K) - \overline{\Phi_N(0)}\Phi_N(0)\Big)$$

ist. Mit dem gleichen Argument wie zuvor, also da $\Phi_N(0)$, $\Phi_N(K)$, b_i und b_{i+1} dem Betrag nach höchstens 1 sind, gilt $|\varepsilon_{K,N}(1)| \leq \frac{2}{K}$. Mit (4.8) gilt

$$|l_r| + |m_r| + |n_r| \quad \leq \quad \frac{1}{q}\sum_{i=0}^{q-1}\left(\left|\overline{a_i}a_{i+r} + \overline{b_i}b_{i+r}\right| + |\overline{a_i}b_{i+r}| + \left|\overline{b_i}a_{i+r}\right|\right)$$

$$
\begin{aligned}
&\leq \frac{1}{q}\sum_{i=0}^{q-1}\left(|\overline{a_i}a_{i+r}| + \left|\overline{b_i}b_{i+r}\right| + |\overline{a_i}b_{i+r}| + \left|\overline{b_i}a_{i+r}\right|\right)\\
&= \frac{1}{q}\sum_{i=0}^{q-1}\left((|a_i| + |b_i|)\left(|a_{i+r}| + |b_{i+r}|\right)\right)\\
&\leq \frac{1}{q}\sum_{i=0}^{q-1}\left(\left(\frac{q-i}{q} + \frac{i}{q}\right)\left(\frac{q-i-r}{q} + \frac{i+r}{q}\right)\right) = 1.
\end{aligned}
$$

□

Lemma 4.7 *Für $r = 0, 1$ gilt*

$$|\Phi^*_{q^2K,q^2N}(r)| \leq p_r|\Phi_{K,N}(0)| + s_r|\Phi_{K,N}(1)| + \frac{7}{K},$$

wobei

$$
\begin{aligned}
p_r &= |l_r\lambda_0 + m_r\lambda_1| + \left|n_r\overline{\lambda_1}\right|,\\
s_r &= |l_r\mu_0 + m_r\mu_1 + n_r\overline{\nu_1}| + |l_r\nu_0 + m_r\nu_1 + n_r\overline{\mu_1}|.
\end{aligned}
$$

Beweis. Mit Lemma 4.6 und Lemma 3.8 erhält man

$$
\begin{aligned}
\Phi^*_{q^2K,q^2N}(r) &= l_r\Phi_{qK,qN}(0) + m_r\Phi_{qK,qN}(1) + n_r\overline{\Phi_{qK,qN}(1)} + \varepsilon_{qK,qN}(r)\\
&= l_r\left(\lambda_0\Phi_{K,N}(0) + \mu_0\Phi_{K,N}(1) + \nu_0\overline{\Phi_{K,N}(1)} + E_{K,N}(0)\right)\\
&\quad + m_r\left(\lambda_1\Phi_{K,N}(0) + \mu_1\Phi_{K,N}(1) + \nu_1\overline{\Phi_{K,N}(1)} + E_{K,N}(1)\right)\\
&\quad + n_r\left(\overline{\lambda_1\Phi_{K,N}(0) + \mu_1\Phi_{K,N}(1) + \nu_1\overline{\Phi_{K,N}(1)} + E_{K,N}(1)}\right)\\
&\quad + \varepsilon_{qK,qN}(r)\\
&= l_r\lambda_0\Phi_{K,N}(0) + l_r\mu_0\Phi_{K,N}(1) + l_r\nu_0\overline{\Phi_{K,N}(1)} + l_rE_{K,N}(0)\\
&\quad + m_r\lambda_1\Phi_{K,N}(0) + m_r\mu_1\Phi_{K,N}(1) + m_r\nu_1\overline{\Phi_{K,N}(1)} + m_rE_{K,N}(1)\\
&\quad + n_r\overline{\lambda_1\Phi_{K,N}(0)} + n_r\overline{\mu_1\Phi_{K,N}(1)} + n_r\overline{\nu_1}\Phi_{K,N}(1) + n_r\overline{E_{K,N}(1)}\\
&\quad + \varepsilon_{qK,qN}(r)
\end{aligned}
$$

$$
\begin{aligned}
&= l_r\lambda_0\Phi_{K,N}(0) + l_r\mu_0\Phi_{K,N}(1) + l_r\nu_0\overline{\Phi_{K,N}(1)} \\
&\quad + m_r\lambda_1\Phi_{K,N}(0) + m_r\mu_1\Phi_{K,N}(1) + m_r\nu_1\overline{\Phi_{K,N}(1)} \\
&\quad + n_r\overline{\lambda_1\Phi_{K,N}(0)} + n_r\overline{\mu_1\Phi_{K,N}(1)} + n_r\overline{\nu_1}\Phi_{K,N}(1) + R_{K,N}(r) \\
&= \left(l_r\lambda_0 + m_r\lambda_1\right)\Phi_{K,N}(0) + n_r\overline{\lambda_1\Phi_{K,N}(0)} \\
&\quad + \left(l_r\mu_0 + m_r\mu_1 + n_r\overline{\nu_1}\right)\Phi_{K,N}(1) \\
&\quad + \left(l_r\nu_0 + m_r\nu_1 + n_r\overline{\mu_1}\right)\overline{\Phi_{K,N}(1)} + R_{K,N}(r)
\end{aligned}
$$

mit $R_{K,N}(r) = l_rE_{K,N}(0) + m_rE_{K,N}(1) + n_r\overline{E_{K,N}(1)} + \varepsilon_{qK,qN}(r)$. Hieraus folgt mit der Dreiecksungleichung

$$\left|\Phi^*_{q^2K,q^2N}(r)\right| \le p_r\left|\Phi_{K,N}(0)\right| + s_r\left|\Phi_{K,N}(1)\right| + \left|R_{K,N}(r)\right|$$

mit p_r und s_r wie oben definiert. Da laut der vorigen beiden Lemmata $|E_{K,N}(r)| \le \frac{2}{K}$, $|\varepsilon_{qK,qN}(r)| \le \frac{2}{qK}$, $|l_r| \le 1$, $|m_r| \le 1$ und $|n_r| \le 1$ gilt, folgt

$$R_{K,N}(r) = \frac{2}{K} + \frac{2}{K} + \frac{2}{K} + \frac{2}{qK} \le \frac{6}{K} + \frac{1}{K} = \frac{7}{K}.$$

□

Lemma 4.8 *Seien $1 \le K \le N$ ganze Zahlen, a_n komplexe Zahlen mit $|a_n| \le 1$, sowie b und m positive ganze Zahlen. Dann gilt*

$$\left|\frac{1}{N}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{N-1} a_n - \frac{1}{K}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{K-1} a_n\right| \le \frac{2(N-K)}{N}.$$

Beweis. Es gilt

$$
\begin{aligned}
&\left|\frac{1}{N}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{N-1} a_n - \frac{1}{K}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{K-1} a_n\right| \\
&\qquad = \left|\frac{1}{N}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{K-1} a_n + \frac{1}{N}\sum_{\substack{n=K\\ n\equiv b \bmod m}}^{N-1} a_n - \frac{1}{K}\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{K-1} a_n\right| \\
&\qquad = \left|\left(\frac{1}{N} - \frac{1}{K}\right)\sum_{\substack{n=0\\ n\equiv b \bmod m}}^{K-1} a_n + \frac{1}{N}\sum_{\substack{n=K\\ n\equiv b \bmod m}}^{N-1} a_n\right|
\end{aligned}
$$

$$
\begin{aligned}
&\leq \left|\frac{1}{N}-\frac{1}{K}\right| \sum_{\substack{n=0 \\ n\equiv b \bmod m}}^{K-1} |a_n| + \frac{1}{N} \sum_{\substack{n=K \\ n\equiv b \bmod m}}^{N-1} |a_n| \\
&\leq \left|\frac{1}{N}-\frac{1}{K}\right| \sum_{n=0}^{K-1} |a_n| + \frac{1}{N} \sum_{n=K}^{N-1} |a_n| \\
&\leq \left|\frac{1}{N}-\frac{1}{K}\right| K + \frac{N-K}{N} = \left|\frac{K-N}{NK}\right| K + \frac{N-K}{N} \\
&= \frac{N-K}{NK} K + \frac{N-K}{N} = \frac{2(N-K)}{N}.
\end{aligned}
$$

□

Nun sind die Voraussetzungen geschaffen, um Proposition 4.4 beweisen zu können.

Beweis von Proposition 4.4. Wie bereits zuvor in (4.6) erwähnt, ist die Behauptung (4.4) äquivalent zu $\Phi^*_{K,N}(0) = \mathcal{O}\left(N^{-\eta}\right)$. Zunächst nehme man an, dass $N \geq q^{20}$ ist. Andernfalls gilt (4.4), wenn man die Konstante des $\mathcal{O}$-Terms entsprechend groß wählt. Setze $t = \left[\frac{\log N}{5 \log q}\right]$, somit gilt

$$
\begin{aligned}
& t \leq \tfrac{\log N}{5 \log q} \\
\Leftrightarrow \quad & \log q^{5t} \leq \log N \\
\Leftrightarrow \quad & q^{5t} \leq N \\
\Leftrightarrow \quad & q^{\frac{5}{2}t} \leq \sqrt{N}.
\end{aligned}
$$

Man nehme nun an, dass $q^{2t+2} \leq \sqrt{N}$ ist. Dies ist der Fall, wenn $2t+2 \leq \frac{5}{2}t$, also wenn $t \geq 4$ ist. Es gilt

$$
t = \left[\frac{\log N}{5 \log q}\right] \geq \left[\frac{\log q^{20}}{5 \log q}\right] = \left[\frac{20 \log q}{5 \log q}\right] = 4.
$$

Damit gilt also $q^{2t+2} \leq \sqrt{N} \leq K \leq N$ und es existieren ganze Zahlen $M \geq 1$, $L \geq 1$ und $0 \leq R, S < q^{2t+2}$ mit $N = q^{t+2}M + R$ und $K = q^{2t+2}L + S$. Mit Lemma 4.8 gilt

für jede positive ganze Zahl k

$$\begin{aligned}
&|\Phi^*_N(k) - \Phi^*_{q^{2t+2}M}(k)| \\
&\quad = \left| \frac{1}{N} \sum_{\substack{n=0 \\ n\equiv v \bmod U}}^{N-1} \overline{g(n)} g(n+k) - \frac{1}{q^{2t+2}M} \sum_{\substack{n=0 \\ n\equiv v \bmod U}}^{q^{2t+2}M-1} \overline{g(n)} g(n+k) \right| \\
&\quad \leq \frac{2(N - q^{2t+2}M)}{N} = \frac{2R}{N} \leq \frac{2q^{2t+2}}{N}.
\end{aligned}$$

Dies liefert

$$\overline{\Phi^*_N(k)}\Phi^*_N(k) = \overline{\Phi^*_{q^{2t+2}M}}(k)\Phi^*_{q^{2t+2}M}(k) + \mathcal{O}\left(\frac{q^{2t}}{N}\right).$$

Also folgt

$$\begin{aligned}
\Phi^*_{K,N}(0) &= \frac{1}{K} \sum_{k=0}^{K-1} \overline{\Phi^*_N(k)}\Phi^*_N(k) \\
&= \frac{1}{K} \sum_{k=0}^{K-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\Phi^*_{q^{2t+2}M}(k) + \mathcal{O}\left(\frac{q^{2t}}{N}\right).
\end{aligned}$$

Laut Lemma 3.5 gilt

$$\begin{aligned}
&\left| \frac{1}{K} \sum_{k=0}^{K-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\ \Phi^*_{q^{2t+2}M}(k) - \frac{1}{q^{2t+2}L} \sum_{k=0}^{q^{2t+2}L-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\Phi^*_{q^{2t+2}M}(k) \right| \\
&\qquad \leq \frac{2(K - q^{2t+2}L)}{K} = \frac{2S}{K} \leq \frac{2q^{2t+2}}{K},
\end{aligned}$$

so dass

$$\frac{1}{K} \sum_{k=0}^{K-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\Phi^*_{q^{2t+2}M}(k) = \frac{1}{q^{2t+2}L} \sum_{k=0}^{q^{2t+2}L-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\Phi^*_{q^{2t+2}M}(k) + \mathcal{O}\left(\frac{q^{2t}}{K}\right).$$

Zusammengefasst gilt also

$$\begin{aligned}
\Phi^*_{K,N}(0) &= \frac{1}{q^{2t+2}L} \sum_{k=0}^{q^{2t+2}L-1} \overline{\Phi^*_{q^{2t+2}M}(k)}\Phi^*_{q^{2t}M}(k) + \mathcal{O}\left(\frac{q^{2t}}{K}\right) + \mathcal{O}\left(\frac{q^{2t}}{N}\right) \\
&= \Phi^*_{q^{2t+2}L,q^{2t+2}M}(0) + \mathcal{O}\left(\frac{q^{2t}}{K}\right) + \mathcal{O}\left(\frac{q^{2t}}{N}\right). \qquad (4.11)
\end{aligned}$$

Laut Lemma 3.9 gilt für $r = 0, 1$ und eine positive ganze Zahl t

$$|\Phi_{q^{2t}L,q^{2t}M}(r)| = |\Phi_{q^{2t}L,q^{2t}M}(r)| \leq e^{-\tau t}\left(1 + \frac{7q^2}{L}\right),$$

mit $\tau = \frac{1}{q^2m^2}$. Hieraus folgt mit Lemma 4.7

$$\begin{aligned}\left|\Phi^*_{q^{2t+2}L,q^{2t+2}M}(0)\right| &= \left|\Phi^*_{q^2q^{2t}L,q^2q^{2t}M}(0)\right| \\ &\leq p_0\left|\Phi_{q^{2t}L,q^{2t}M}(0)\right| + s_0\left|\Phi_{q^{2t}L,q^{2t}M}(1)\right| + \frac{7}{q^{2t}L} \\ &\leq (p_0+s_0)e^{-\tau t}\left(1+\frac{7q^2}{L}\right) + \frac{7}{q^{2t}L}.\end{aligned}$$

Da die Koeffizienten aus den Lemmata 4.6 und 3.8, aus denen sich p_0 und s_0 zusammensetzen, vom Betrag höchstens 1 sind, gilt $|p_0 - s_0| \leq 9$, $|p_0 - s_0|$ ist also beschränkt. Des weiteren ist $1 + \frac{7q^2}{L}$ beschränkt, da q eine feste positive ganze Zahl und $L \geq 1$ ist. Insgesamt erhält man also

$$\Phi^*_{K,N}(0) = \mathcal{O}\left(e^{-\tau t}\right) + \mathcal{O}\left(\frac{q^{2t}}{\sqrt{N}}\right) + \mathcal{O}\left(\frac{1}{q^{2t}L}\right), \tag{4.12}$$

wobei die Konstante des $\mathcal{O}$-Terms des ersten Summanden nur von q abhängt und sich der zweite Summand aus der Zusammenfassung der beiden Fehlerterme der Abschätzung (4.11) mit Hilfe der Ungleichung $\sqrt{N} \leq K \leq N$ ergibt. Aufgrund der Definition von t gilt

$$\frac{\log N}{5\log q} - 1 \leq t \leq \frac{\log N}{5\log q} \tag{4.13}$$

und damit

$$t \geq \frac{\log N}{5\log q} - 1 = \frac{2\log N - \log q^{10}}{10\log q} \geq \frac{\frac{3}{2}\log N}{10\log q} \geq \frac{\log N}{10\log q}.$$

Dies impliziert

$$-\tau t \leq -\tau\frac{\log N}{10\log q} = -\tau\frac{\log N}{10\log q} = -\frac{\log N}{10q^2m^2\log q} \leq -\frac{\log N}{10q^3m^2}$$

und somit gilt $e^{-\tau t} \leq N^{-\frac{1}{10q^3m^2}}$. Außerdem erhält man aus Ungleichung (4.13)

$$\begin{aligned}t \leq \frac{\log N}{5\log q} &\Leftrightarrow 2t\log q \leq \frac{2}{5}\log N \\ &\Leftrightarrow \log q^{2t} \leq \frac{2}{5}\log N \\ &\Leftrightarrow q^{2t} \leq \exp\left(\frac{2}{5}\log N\right)\end{aligned}$$

womit

$$\frac{q^{2t}}{\sqrt{N}} \leq \frac{1}{\sqrt{N}} \exp\left(\frac{2}{5}\log N\right) = N^{-\frac{1}{10}}$$

gilt. Ebenfalls mit der Ungleichung (4.13) gilt

$$\begin{aligned} t \geq \frac{\log N}{10 \log q} &\Leftrightarrow t \log q \geq \frac{\log N}{10} \\ &\Leftrightarrow -\log q^{2t} \leq -\frac{2}{10}\log N \\ &\Leftrightarrow \log \frac{1}{q^{2t}} \leq -\frac{1}{5}\log N \\ &\Leftrightarrow \frac{1}{q^{2t}} \leq \exp\left(-\frac{1}{5}\log N\right) \end{aligned}$$

und man erhält bezüglich des dritten Summanden in (4.12)

$$\frac{1}{q^{2t}L} \leq \frac{1}{q^{2t}} \leq \exp\left(-\frac{1}{5}\log N\right) = N^{-\frac{1}{5}}.$$

Mit $\eta = \frac{1}{10q^3m^2}$ sind die Fehlerterme aus (4.12) von der Ordnung $\mathcal{O}(N^{-\eta})$ und damit folgt die Behauptung. □

Proposition 4.4 wird nun verwendet, um die folgende Proposition zu beweisen, welche im Beweis von Satz 4.2 den Fehlerterm der Abschätzung liefern wird.

Proposition 4.9 *Die l-Tupel $\mathbf{m}$, $\mathbf{q}$, $\mathbf{f}$, $\mathbf{u}$ und $\mathbf{v}$ seien wie im ersten Abschnitt des Kapitels gegeben, $\mathbf{h} = (h_1, h_2, \ldots, h_l)$ sei ein l-Tupel aus ganzen Zahlen, so dass $m_i \nmid d_i h_i$ für mindestens einen Index i gilt. Dann gilt für alle positiven ganzen Zahlen N*

$$\sum_{n=0}^{N-1} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} f_j\left(u_j n + v_j\right)\right) = \mathcal{O}\left(N^{1-\delta}\right), \tag{4.14}$$

wobei $\delta = \frac{1}{120l^2\overline{q}^3\overline{m}^2}$ ist und die $\mathcal{O}$-Konstante nur von $\mathbf{q}, \mathbf{u}$ und l abhängt.

Beweis. Setze $g_j(x) = e\left(\frac{h_j}{m_j} f_j(x)\right)$ und $g(\mathbf{u}n + \mathbf{v}) = \prod_{j=1}^{l} g_j(u_j n + v_j)$. Dann gilt

$$\sum_{n=0}^{N-1} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} f_j(u_j n + v_j)\right) = \sum_{n=0}^{N-1} \prod_{j=1}^{l} e\left(\frac{h_j}{m_j} f_j(u_j n + v_j)\right)$$

$$
\begin{aligned}
&= \sum_{n=0}^{N-1} \prod_{j=1}^{l} g_j(u_j n + v_j) \\
&= \sum_{n=0}^{N-1} g(\mathbf{u}n + \mathbf{v})
\end{aligned}
$$

und die Aussage (4.14) lässt sich schreiben als

$$\left| \sum_{n=0}^{N-1} g(\mathbf{u}n + \mathbf{v}) \right| = \mathcal{O}\left(N^{1-\delta}\right). \tag{4.15}$$

Gegeben sei eine positive ganze Zahl N, setze $K = \left[\frac{N^{\frac{1}{3l}}}{\overline{u}}\right]$. Mit Lemma 2.4 gilt dann

$$\left| \sum_{n=0}^{N-1} g(\mathbf{u}n + \mathbf{v}) \right|^2 \leq \frac{2N^2}{K} + \frac{4N}{K} \sum_{k=1}^{K} \left| \sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \right| \tag{4.16}$$

im Fall $1 \leq K \leq N$. Setze $t_j = \left[\frac{2 \log \overline{u}K}{\log q_j}\right]$ und $Q_j = q_j^{t_j}$. Dann gilt $\frac{(\overline{u}K)^2}{q_j} \leq Q_j \leq (\overline{u}K)^2$, denn

$$
\begin{aligned}
& \tfrac{2 \log \overline{u}K}{\log q_j} - 1 \quad \leq t_j \leq \quad \tfrac{2 \log \overline{u}K}{\log q_j} \\
\Leftrightarrow \quad & 2 \log \overline{u}K - \log q_j \leq t_j \log q_j \leq 2 \log \overline{u}K \\
\Leftrightarrow \quad & \log \tfrac{(\overline{u}K)^2}{q_j} \leq \log q_j^{t_j} \leq \log(\overline{u}K)^2 \\
\Leftrightarrow \quad & \tfrac{(\overline{u}K)^2}{q_j} \quad \leq q_j^{t_j} \leq \quad (\overline{u}K)^2.
\end{aligned}
$$

Setze $N \geq (\overline{qu})^{3l}$, da für $1 \leq N < (\overline{qu})^{3l}$ die Abschätzung (4.15) erfüllt ist, wenn man die Konstante des $\mathcal{O}$-Terms groß genug wählt. Damit ist $K \geq \overline{q}$ und es gilt $\overline{u}K \geq \overline{uq} \geq q_j$. Hieraus folgt zum einen $t_j \geq 2$ und zum anderen

$$2 \leq \overline{u}K \leq \frac{(\overline{u}K)^2}{q_j} \leq Q_j \leq (\overline{u}K)^2. \tag{4.17}$$

Sei nun $\mathbf{Q} = (Q_1, Q_2, \ldots, Q_l)$. Zu einem gegebenen l-Tupel $\mathbf{r} = (r_1, r_2, \ldots, r_l)$ definiere man

$$P_{\mathbf{r}} = \{n \in \mathbb{N}_0 : n \equiv \mathbf{r} \bmod \mathbf{Q}\},$$

wobei die Kongruenz so zu verstehen ist, dass sie komponentenweise gilt. Da die q_j und damit auch die Q_j paarweise teilerfremd sind, ist das obige Kongruenzsystem äquivalent zu einer einzelnen Kongruenz modulo $\prod_{j=1}^{l} Q_j$. Damit erhält man

$$|\{0 \leq n \leq N : n \in P_{\mathbf{r}}\}| = \frac{N}{\prod_{j=1}^{l} Q_j} + \mathcal{O}(1). \tag{4.18}$$

Setze $\mathcal{R} = \{\mathbf{r} = (r_1, r_2, \ldots, r_l) : 0 \leq r_j \leq Q_j - 1 \text{ für } j = 1, \ldots, l\}$ und definiere zu einem gegebenen l-Tupel $\mathbf{s} = (s_1, s_2, \ldots, s_l)$

$$\widehat{P}_{\mathbf{s}} = \{\mathbf{r} \in \mathcal{R} : \mathbf{ur} + \mathbf{v} \equiv \mathbf{s} \bmod \mathbf{Q}\}.$$

Die Kongruenz $u_j r_j + v_j \equiv s_j \bmod Q_j$ besitzt, falls sie lösbar ist, genau (u_j, Q_j) verschiedene Lösungen modulo Q_j. Aus diesem Grund sowie aufgrund der Definition von u_j gilt

$$\left|\widehat{P}_{\mathbf{s}}\right| = \frac{|\mathcal{R}| \prod_{j=1}^{l}(u_j, Q_j)}{\prod_{j=1}^{l} Q_j} = \prod_{j=1}^{l}(u_j, Q_j) = \prod_{j=1}^{l}(u_j, q_j^{t_j}) = \prod_{j=1}^{l}(u_j, q_j) \leq \overline{q}^l$$

für den Fall, dass das Kongruenzsystem lösbar ist. Dies ist genau dann der Fall, wenn für $j = 1, \ldots, l$ die Aussage $(u_j, Q_j) | (s_j - v_j)$ gilt. Diese Bedingung lässt sich in $v_j \equiv s_j \bmod (u_j, q_j)$ umformulieren, da laut Voraussetzung $(u_j, Q_j) = (u_j, q_j)$ gilt. Des weiteren werden definiert

$$\begin{aligned}
\mathcal{S} = \{&\mathbf{s} = (s_1, s_2, \ldots, s_l) : 0 \leq s_j \leq Q_j - 1 \text{ so dass} \\
&\exists \mathbf{r} \in \mathcal{R} \text{ mit } \mathbf{ur} + \mathbf{v} \equiv \mathbf{s} \bmod \mathbf{Q}\} \\
\mathcal{S}_0 = \{&\mathbf{s} = (s_1, s_2, \ldots, s_l) : 0 \leq s_j \leq Q_j - u_j K - 1 \text{ so dass} \\
&\exists \mathbf{r} \in \mathcal{R} \text{ mit } \mathbf{ur} + \mathbf{v} \equiv \mathbf{s} \bmod \mathbf{Q}\}.
\end{aligned}$$

Betrachte nun die innere Summe der rechten Seite von (4.16). Für $1 \leq k \leq K$ gilt

$$\begin{aligned}
&\sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \sum_{\mathbf{r} \in \mathcal{R}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \sum_{\mathbf{s} \in \mathcal{S}} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \sum_{\mathbf{s} \in \mathcal{S}_0} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad\quad + \sum_{\mathbf{s} \in \mathcal{S} \setminus \mathcal{S}_0} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k).
\end{aligned} \tag{4.19}$$

Wenn $\mathbf{s} \in \mathcal{S}_0$, $n \in P_{\mathbf{r}}$ und $\mathbf{r} \in \widehat{P}_{\mathbf{s}}$, so folgt $n \equiv r_j \bmod Q_j$, $u_j r_j + v_j \equiv s_j \bmod Q_j$ und $0 \leq s_j + u_j k < Q_j$ für alle $j = 1, \ldots, l$ und $k = 1, \ldots, K$. Damit folgt in diesem Fall aus Lemma 4.3 und da $\overline{e(x)} = e(-x)$ für reelle Zahlen x gilt

$$\begin{aligned}
&\overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \prod_{j=1}^{l} \overline{g_j(u_j n + v_j)} g_j(u_j n + v_j + u_j k) \\
&\qquad = e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} \left(f_j(u_j n + v_j + u_j k) - f_j(u_j n + v_j) \right) \right) \\
&\qquad = e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} \left(f_j(s_j + u_j k) - f_j(s_j) \right) \right) \\
&\qquad = \prod_{j=1}^{l} \overline{g_j(s_j)} g_j(s_j + u_j k).
\end{aligned}$$

Daher gilt für die erste Dreifachsumme in (4.19)

$$\begin{aligned}
&\sum_{\mathbf{s} \in \mathcal{S}_0} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \sum_{\mathbf{s} \in \mathcal{S}_0} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \prod_{j=1}^{l} \overline{g_j(s_j)} g_j(s_j + u_j k) \\
&\qquad = \sum_{\mathbf{s} \in \mathcal{S}} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \prod_{j=1}^{l} \overline{g_j(s_j)} g_j(s_j + u_j k) \\
&\qquad\quad - \sum_{\mathbf{s} \in \mathcal{S} \setminus \mathcal{S}_0} \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} \prod_{j=1}^{l} \overline{g_j(s_j)} g_j(s_j + u_j k)
\end{aligned}$$

und somit erhält man

$$\begin{aligned}
&\sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n + \mathbf{v})} g(\mathbf{u}n + \mathbf{v} + \mathbf{u}k) \\
&\qquad = \sum_{\mathbf{s} \in \mathcal{S}} \prod_{j=1}^{l} \overline{g_j(s_j)} g_j(s_j + u_j k) \sum_{\mathbf{r} \in \widehat{P_{\mathbf{s}}}} \sum_{\substack{n=0 \\ n \in P_{\mathbf{r}}}}^{N-k-1} 1
\end{aligned}$$

$$+\sum_{\mathbf{s}\in\mathcal{S}\setminus\mathcal{S}_0}\sum_{\mathbf{r}\in\widehat{P_{\mathbf{s}}}}\sum_{\substack{n=0\\ n\in P_{\mathbf{r}}}}^{N-k-1}\left(\overline{g(\mathbf{u}n+\mathbf{v})}g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k)-\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\right)$$
$$=:\sum\nolimits_1+\sum\nolimits_2.$$

Nun wird $\sum_2$ mit (4.18) sowie den trivialen Schranken $|g_j(x)|\le 1$ und $|g(x)|\le 1$ abgeschätzt. Außerdem wird die folgende Abschätzung benötigt. Es gilt

$$\begin{aligned}
|\mathcal{S}\setminus\mathcal{S}_0| &\le \sum_{i=1}^{l}|\{\mathbf{s}: 0\le s_j\le Q_j-1,\, Q_i-u_iK\le s_i\le Q_i-1 \text{ für } i\ne j,\\
&\qquad\qquad \exists\mathbf{r}\in\mathcal{R} \text{ mit } \mathbf{ur}+\mathbf{v}\equiv\mathbf{s} \bmod \mathbf{Q}\}|\\
&\le \sum_{i=1}^{l}|\{\mathbf{s}: 0\le s_j\le Q_j-1,\, Q_i-u_iK\le s_i\le Q_i-1 \text{ für } i\ne j\}|\\
&\le \sum_{i=1}^{l}\left(\overline{u}K\prod_{\substack{j=1\\ i\ne j}}^{l}Q_j\right)\le\sum_{i=1}^{l}\left(\frac{\overline{u}K}{Q_i}\prod_{j=1}^{l}Q_j\right)\\
&\le \left(\prod_{j=1}^{l}Q_j\right)\frac{1}{\overline{u}K}\sum_{i=1}^{l}q_i\le\frac{\overline{q}l}{\overline{u}K}\prod_{j=1}^{l}Q_j,
\end{aligned}$$

wobei die vorletzte Ungleichung direkt aus $\frac{(\overline{u}K)^2}{q_j}\le Q_j$ folgt (siehe (4.17)). Mit $\left|\widehat{P}_{\mathbf{s}}\right|\le\overline{q}^l$ und (4.18) erhält man somit

$$\begin{aligned}
&|\textstyle\sum_2|\\
&= \left|\sum_{\mathbf{s}\in\mathcal{S}\setminus\mathcal{S}_0}\sum_{\mathbf{r}\in\widehat{P_{\mathbf{s}}}}\sum_{\substack{n=0\\ n\in P_{\mathbf{r}}}}^{N-k-1}\left(\overline{g(\mathbf{u}n+\mathbf{v})}g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k)-\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\right)\right|\\
&\le \sum_{\mathbf{s}\in\mathcal{S}\setminus\mathcal{S}_0}\sum_{\mathbf{r}\in\widehat{P_{\mathbf{s}}}}\sum_{\substack{n=0\\ n\in P_{\mathbf{r}}}}^{N-k-1}\left(\left|\overline{g(\mathbf{u}n+\mathbf{v})}g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k)\right|+\left|\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\right|\right)\\
&\le \sum_{\mathbf{s}\in\mathcal{S}\setminus\mathcal{S}_0}\sum_{\mathbf{r}\in\widehat{P_{\mathbf{s}}}}\sum_{\substack{n=0\\ n\in P_{\mathbf{r}}}}^{N-k-1}2\le 2|\mathcal{S}\setminus\mathcal{S}_0||\widehat{P}_{\mathbf{s}}|\left(\frac{N-k-1}{\prod_{j=1}^{l}Q_j}+\mathcal{O}(1)\right)\\
&\le \frac{2l\overline{q}^{l+1}}{\overline{u}K}\prod_{j=1}^{l}Q_j\left(\frac{N-k-1}{\prod_{j=1}^{l}Q_j}+\mathcal{O}(1)\right)
\end{aligned}$$

$$\begin{aligned} &\leq \frac{2l\overline{q}^{l+1}}{\overline{u}K}(N-k-1)+\mathcal{O}\left(\frac{1}{K}\prod_{j=1}^{l}Q_j\right)\\ &\leq 2l\overline{q}^{l+1}\frac{N}{\overline{u}K}+\mathcal{O}\left(\frac{1}{K}\prod_{j=1}^{l}Q_j\right). \end{aligned} \tag{4.20}$$

Für $\sum_1$ wird wiederum (4.18) sowie $\left|\widehat{P}_{\mathbf{s}}\right| = \prod_{j=1}^{l}(u_j,q_j)$ und $(u_j,q_j)\leq\overline{q}^l$ verwendet. Es gilt

$$\begin{aligned} &\sum\nolimits_1\\ &= \sum_{\mathbf{s}\in\mathcal{S}}\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\sum_{\mathbf{r}\in\widehat{P_{\mathbf{s}}}}\sum_{\substack{n=0\\ n\in P_{\mathbf{r}}}}^{N-k-1}1\\ &= \sum_{\mathbf{s}\in\mathcal{S}}\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\prod_{i=1}^{l}(u_i,Q_i)\left(\frac{N-k-1}{\prod_{m=1}^{l}Q_m}+\mathcal{O}(1)\right)\\ &= \prod_{i=1}^{l}(u_i,q_i)\left(\frac{N-k-1}{\prod_{m=1}^{l}Q_m}+\mathcal{O}(1)\right)\sum_{\mathbf{s}\in\mathcal{S}}\prod_{j=1}^{l}\overline{g_j(s_j)}g_j(s_j+u_jk)\\ &= \prod_{i=1}^{l}(u_i,q_i)\left(\frac{N-k-1}{\prod_{m=1}^{l}Q_m}+\mathcal{O}(1)\right)\prod_{j=1}^{l}\left(\sum_{\substack{s_j=0\\ s_j\equiv v_j \bmod (u_j,q_j)}}^{Q_j-1}\overline{g_j(s_j)}g_j(s_j+u_jk)\right)\\ &\leq (N-k-1)\prod_{i=1}^{l}\frac{(u_i,q_i)}{Q_i}\prod_{j=1}^{l}\left(\sum_{\substack{s_j=0\\ s_j\equiv v_j \bmod (u_j,q_j)}}^{Q_j-1}\overline{g_j(s_j)}g_j(s_j+u_jk)\right)\\ &\quad+\mathcal{O}\left(\prod_{i=1}^{l}(u_i,q_i)\prod_{j=1}^{l}\left(\sum_{\substack{s_j=0\\ s_j\equiv v_j \bmod (u_j,q_j)}}^{Q_j-1}1\right)\right)\\ &= (N-k-1)\prod_{i=1}^{l}\frac{(u_i,q_i)}{Q_i}\prod_{j=1}^{l}\left(\sum_{\substack{s_j=0\\ s_j\equiv v_j \bmod (u_j,q_j)}}^{Q_j-1}\overline{g_j(s_j)}g_j(s_j+u_jk)\right)\\ &\quad+\mathcal{O}\left(\prod_{i=1}^{l}Q_i\right). \end{aligned} \tag{4.21}$$

Aus (4.17) und der Definition von K folgt $\prod_{i=1}^{l}Q_i\leq(\overline{u}K)^{2l}\leq\left(\frac{\overline{u}N^{\frac{1}{3l}}}{\overline{u}}\right)^{2l}=N^{\frac{2}{3}}\leq\overline{u}N^{1-\frac{1}{3l}}\leq\frac{N}{K}$. Damit sind die rechte Seite in (4.20) und der Fehlerterm in (4.21) von

der Ordnung $\frac{N}{K}$. Fasst man zusammen, so gilt also

$$\begin{aligned}
&\sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n+\mathbf{v})} g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k) \\
= \;& (N-k-1) \prod_{i=1}^{l} \frac{(u_i,q_i)}{Q_i} \prod_{j=1}^{l} \left(\sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right) \\
+ \;& \mathcal{O}\left(\frac{N}{K}\right).
\end{aligned}$$

Mit (4.16) folgt daraus

$$\begin{aligned}
&\left| \sum_{n=0}^{N-1} g(\mathbf{u}n+\mathbf{v}) \right|^2 \\
&\qquad \leq \frac{2N^2}{K} + \frac{4N}{K} \sum_{k=1}^{K} \left| \sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n+\mathbf{v})} g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k) \right| \\
&\qquad = \frac{4N}{K} \sum_{k=1}^{K} \left| \sum_{n=0}^{N-k-1} \overline{g(\mathbf{u}n+\mathbf{v})} g(\mathbf{u}n+\mathbf{v}+\mathbf{u}k) \right| + \mathcal{O}\left(\frac{N^2}{K}\right) \\
&\qquad \leq \frac{4N^2}{K} \sum_{k=1}^{K} \left| \prod_{i=1}^{l} \frac{(u_i,q_i)}{Q_i} \prod_{j=1}^{l} \left(\sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right) \right| \\
&\qquad + \;\; \mathcal{O}\left(\frac{N^2}{K}\right) \\
&\qquad \leq \frac{4N^2\overline{q}^l}{K} \sum_{k=1}^{K} \left| \prod_{i=1}^{l} \frac{1}{Q_i} \prod_{j=1}^{l} \left(\sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right) \right| \\
&\qquad + \;\; \mathcal{O}\left(\frac{N^2}{K}\right) \\
&\qquad =: \frac{4N^2\overline{q}^l}{K} \sum\nolimits_3 + \mathcal{O}\left(\frac{N^2}{K}\right).
\end{aligned}$$

Für die Abschätzung von $\sum_3$ wird zunächst die Hölder-Ungleichung verwendet. Es gilt

$$
\begin{aligned}
&\sum\nolimits_3 \\
&\quad= \sum_{k=1}^{K} \left| \prod_{j=1}^{l} \left(\frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right) \right| \\
&\quad= \sum_{k=1}^{K} \left| 1 \cdot \prod_{j=1}^{l} \left(\frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right) \right| \\
&\quad\le \left(\sum_{k=1}^{K} 1^{l+1} \right)^{\frac{1}{l+1}} \prod_{j=1}^{l} \left(\sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right|^{l+1} \right)^{\frac{1}{l+1}} \\
&\quad= K^{\frac{1}{l+1}} \prod_{j=1}^{l} \left(\sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right|^{l+1} \right)^{\frac{1}{l+1}} \\
&\quad= K \prod_{j=1}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right|^{l+1} \right)^{\frac{1}{l+1}} \\
&\quad\le K \prod_{j=1}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right|^{2} \right)^{\frac{1}{l+1}} \\
&\quad= K \prod_{\substack{j=1 \\ j\neq i}}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_jk) \right|^{2} \right)^{\frac{1}{l+1}} \\
&\qquad\cdot \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+u_ik) \right|^{2} \right)^{\frac{1}{l+1}},
\end{aligned}
\tag{4.22}
$$

wobei ausgenutzt wurde, dass

$$\left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_j k) \right| \leq 1$$

ist. Der zweite Faktor in (4.22) wiederum lässt sich durch

$$\begin{aligned} &\left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+u_i k) \right|^2 \right)^{\frac{1}{l+1}} \\ &\qquad \leq \left(\frac{1}{K} \sum_{k'=1}^{u_i K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+k') \right|^2 \right)^{\frac{1}{l+1}} \\ &\qquad \leq \left(\frac{1}{K} \sum_{k'=1}^{\overline{u}K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+k') \right|^2 \right)^{\frac{1}{l+1}} \end{aligned} \tag{4.23}$$

abschätzen, wobei $u_i k = k'$ gesetzt wurde. Damit ergibt sich insgesamt

$$\begin{aligned} &\sum\nolimits_3 \\ &\quad \leq K \prod_{\substack{j=1 \\ j \neq i}}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_j k) \right|^2 \right)^{\frac{1}{l+1}} \\ &\qquad \cdot \left(\frac{1}{K} \sum_{k'=1}^{\overline{u}K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+k') \right|^2 \right)^{\frac{1}{l+1}} \\ &\quad = \overline{u}^{\frac{1}{l+1}} K \prod_{\substack{j=1 \\ j \neq i}}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{\substack{s_j=0 \\ s_j \equiv v_j \bmod (u_j,q_j)}}^{Q_j-1} \overline{g_j(s_j)} g_j(s_j+u_j k) \right|^2 \right)^{\frac{1}{l+1}} \\ &\qquad \cdot \left(\frac{1}{\overline{u}K} \sum_{k'=1}^{\overline{u}K} \left| \frac{1}{Q_i} \sum_{\substack{s_i=0 \\ s_i \equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} \overline{g_i(s_i)} g_i(s_i+k') \right|^2 \right)^{\frac{1}{l+1}} . \end{aligned} \tag{4.24}$$

Laut Voraussetzung der Proposition gilt $m_j \nmid d_j h_j$ für mindestens einen Index j. Sei dies der Index i aus (4.23). Um nun Proposition 4.4 anwenden zu können, muss $\sqrt{Q_i} \leq \overline{u}K \leq Q_i$ gezeigt werden. Laut (4.17) gilt $\overline{u}K \leq Q_j$ und $Q_j \leq (\overline{u}K)^2$. Ziehen der Wurzel in der zweiten Ungleichung führt zu dem gewünschten Ergebnis. Damit gilt laut Proposition 4.4

$$\begin{aligned}
&\frac{1}{\overline{u}K}\sum_{k'=1}^{\overline{u}K}\left|\frac{1}{Q_i}\sum_{\substack{s_i=0\\ s_i\equiv v_i \bmod (u_i,q_i)}}^{Q_i-1}\overline{g_i(s_i)}g_i(s_i+k')\right|^2 \\
&\qquad = \frac{1}{\overline{u}K}\sum_{k'=1}^{\overline{u}K}\left|\frac{1}{Q_i}\sum_{\substack{s_i=0\\ s_i\equiv v_i \bmod (u_i,q_i)}}^{Q_i-1} e\left(\frac{h_i}{m_i}\left(f_i(s_i+k')-f(s_i)\right)\right)\right|^2 \\
&\qquad = \mathcal{O}\left(Q_i^{-\eta_i}\right) = \mathcal{O}\left((\overline{u}K)^{-\eta_i}\right),
\end{aligned}$$

wobei $\eta_i = \frac{1}{10q_i^3 m_i^2}$ und die Konstante des $\mathcal{O}$-Terms nur von q_i abhängt.

Sei $x \geq 2$ eine reelle Zahl. Dann gilt

$$\frac{1}{2}x \geq \{x\} \;\Leftrightarrow\; \frac{1}{2}x - \{x\} \geq 0 \;\Leftrightarrow\; x - \{x\} \geq \frac{1}{2}x \;\Leftrightarrow\; [x] \geq \frac{1}{2}x, \tag{4.25}$$

da $\{x\} \leq 1$ ist. Mit der Annahme, dass $N \geq (\overline{qu})^{3l}$ ist, gilt $N^{\frac{1}{3l}} \geq \overline{qu} \geq 2\overline{u}$, woraus folgt, dass $\frac{N^{\frac{1}{3l}}}{2\overline{u}} \geq 1$. Somit folgt $K = \left[\frac{N^{\frac{1}{3l}}}{\overline{u}}\right] \geq \frac{N^{\frac{1}{3l}}}{2\overline{u}}$ mit (4.25). Setzt man $\eta = \frac{1}{10\overline{q}^3\overline{m}^2}$, so ist $\eta \leq \eta_i$ und

$$(\overline{u}K)^{-\eta_i} \leq (\overline{u}K)^{-\eta} \leq 2^{\eta}\left(N^{\frac{1}{3l}}\right)^{-\eta} = 2^{\eta}N^{\frac{-\eta}{3l}} \leq 2N^{\frac{-\eta}{3l}}.$$

Es gilt also

$$\frac{1}{\overline{u}K}\sum_{k'=1}^{\overline{u}K}\left|\frac{1}{Q_i}\sum_{\substack{s_i=0\\ s_i\equiv v_i \bmod (u_i,q_i)}}^{Q_i-1}\overline{g_i(s_i)}g_i(s_i+k')\right|^2 = \mathcal{O}\left(N^{\frac{-\eta}{3l}}\right).$$

Die übrigen Faktoren in (4.24) werden mit 1 abgeschätzt, so dass

$$\sum_3 = \mathcal{O}\left(KN^{\frac{-\eta}{3l(l+1)}}\right) = \mathcal{O}\left(KN^{\frac{-\eta}{6l^2}}\right)$$

gilt. Schließlich erhält man für (4.16)

$$\left|\sum_{n=0}^{N-1} g(\mathbf{u}n+\mathbf{v})\right|^2 = \frac{4N^2\overline{q}^l}{K}\sum\nolimits_3 + \mathcal{O}\left(\frac{N^2}{K}\right) = \mathcal{O}\left(N^{2-\frac{\eta}{6l^2}}\right) + \mathcal{O}\left(N^{2-\frac{1}{3l}}\right).$$

Da $\delta = \frac{1}{120l^2q^3m^2} = \frac{\eta}{12l^2}$ ist, sind die Exponenten in den Fehlertermen $\leq 2 - 2\delta$ und die Proposition ist bewiesen. □

Das folgende Lemma ist eine allgemeinere Version des Chinesischen Restsatzes. Der Beweis ist nachzulesen in [19].

Lemma 4.10 [19, Theorem 5.4.3] *Das Kongruenzsystem*

$$a_i x \equiv b_i \bmod m_i \quad (i = 1, \ldots, k)$$

hat genau dann eine Lösung, wenn für alle $i, j \in \{1, \ldots, k\}$

$$d_i = (a_i, m_i) | b_i \quad \textit{und} \quad \Delta_{ij} = \frac{b_j a_i - b_i a_j}{d_i d_j} \equiv 0 \bmod \left(\frac{m_i}{d_i}, \frac{m_j}{d_j} \right)$$

gilt. Die Lösungen sind dann eindeutig modulo $kgV\left(\frac{m_1}{d_1}, \ldots, \frac{m_k}{d_k}\right)$.

Dieses Lemma ist ein wichtiges Hilfsmittel, um das folgende Lemma zu beweisen.

Lemma 4.11 *Seien* $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{f}$, $\mathbf{F}$ *und* $\mathbf{d}$ *wie im ersten Abschnitt des Kapitels definiert.*

(i) Ein l*-Tupel* $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ *aus ganzen Zahlen ist genau dann zulässig bezüglich* $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ *und* $\mathbf{f}$, *wenn*

$$(u_j F_j, d_j) | (a_j - v_j F_j) \qquad (1 \leq j \leq l), \tag{4.26}$$

$$a_i^* F_j^* \equiv a_j^* F_i^* \bmod (d_i^*, d_j^*) \qquad (i \neq j), \tag{4.27}$$

wobei $a_j^* = \frac{a_j - v_j F_j}{(u_j F_j, d_j)}$, $F_j^* = \frac{u_j F_j}{(u_j F_j, d_j)}$ *und* $d_j^* = \frac{d_j}{(u_j F_j, d_j)}$ *seien.*

(ii) Wenn $\mathbf{a}$ *zulässig ist, so gilt*

$$|\{0 \leq n < N : (\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}\}| = \begin{cases} \frac{N}{D} + \mathcal{O}(1) & \textit{für } N \geq 1 \\ \frac{N}{D} & \textit{falls } D | N \end{cases}, \tag{4.28}$$

wobei $D = kgV(d_1^*, d_2^*, \ldots, d_l^*)$ *sei.*

(iii) Die Menge $\mathcal{A}$ der bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ *und* $\mathbf{f}$ *zulässigen l-Tupel genügt der Gleichung*

$$|\mathcal{A}| = \left(\prod_{j=1}^{l} \frac{m_j}{d_j} \right) D. \tag{4.29}$$

Beweis. Sei $\mathbf{a}$ zulässig bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$. Dies ist laut Definition genau dann der Fall, wenn das Kongruenzsystem $(\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}$ eine Lösung besitzt. Dieses Kongruenzsystem ist wiederum äquivalent zu $\mathbf{u}n\mathbf{F} \equiv \mathbf{a} - \mathbf{v}\mathbf{F} \bmod \mathbf{d}$. Laut des Allgemeinen Chinesischen Restsatzes, Lemma 4.10, besitzt dieses Kongruenzsystem genau dann eine Lösung, wenn die Gleichungen (4.26) und (4.27) erfüllt sind. Ebenfalls laut des Allgemeinen Chinesischen Restsatzes ist die Lösung des Kongruenzsystems eindeutig mod D und es folgt die Gleichung (4.28). Nun ist noch (iii) zu zeigen. Man definiere

$$\mathcal{A}^* = \big\{ \mathbf{a} = (a_1, a_2, \ldots, a_l) : 0 \le a_j \le d_j - 1 \ (1 \le j \le l), \\ \mathbf{a} \text{ zulässig bzgl. } \mathbf{q}, \mathbf{m}, \mathbf{u}, \mathbf{v} \text{ und } \mathbf{f} \big\}.$$

Ist ein Tupel $\mathbf{a}^* = (a_1^*, \ldots, a_l^*) \in \mathcal{A}^*$ gegeben, so ist laut Definition jedes Tupel der Form $\mathbf{a} = (a_1^* + k_1 d_1, \ldots, a_l^* + k_l d_l)$, wobei $k_1, \ldots, k_l$ ganze Zahlen seien, ebenfalls zulässig bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$. Ist ferner $0 \le k_j \le \frac{m_j}{d_j}$ für alle j, so gilt für die Einträge von $\mathbf{a}$ die Abschätzung $0 \le a_j < m_j$ $(1 \le j \le l)$, womit $\mathbf{a}$ ein Element der Menge $\mathcal{A}$ ist. Daher korrespondieren zu jedem $\mathbf{a}^* \in \mathcal{A}^*$ genau $\prod_{j=1}^{l} \left(\frac{m_j}{d_j} \right)$ dieser Tupel $\mathbf{a}$. Ist umgekehrt ein $\mathbf{a} \in \mathcal{A}$ gegeben, so existiert ein eindeutiges Tupel $\mathbf{a}^* \in \mathcal{A}^*$, so dass $\mathbf{a}$ von der obigen Form ist. Daher gilt

$$|\mathcal{A}| = \prod_{j=1}^{l} \left(\frac{m_j}{d_j} \right) |\mathcal{A}^*|$$

und es genügt zum Beweis von (4.29), zu zeigen, dass

$$|\mathcal{A}^*| = D$$

ist. Sei dazu ein beliebiges Tupel $\mathbf{a} = (a_1, \ldots, a_l)$ mit $0 \le a_j < d_j$ $(1 \le j \le l)$ gegeben und sei

$$\mathcal{N}(\mathbf{a}) = \left\{ 0 \le n < \prod_{j=1}^{l} d_j : (\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d} \right\}.$$

Da $D = kgV(d_1^*, d_2^*, \ldots, d_l^*)$ ist, teilt D das Produkt $\prod_{j=1}^{l} \frac{d_j}{(u_j F_j, d_j)}$ und damit auch das Vielfache $\prod_{j=1}^{l} d_j$. Damit folgt aus Teil (ii) des Lemmas

$$|\mathcal{N}(\mathbf{a})| = \begin{cases} \frac{\prod_{j=1}^{l} d_j}{D} & \text{falls } \mathbf{a} \in \mathcal{A}^*, \\ 0 & \text{sonst} \end{cases}$$

und es gilt

$$\sum_{\mathbf{a} \bmod \mathbf{d}} |\mathcal{N}(\mathbf{a})| = |\mathcal{A}^*| \frac{\prod_{j=1}^{l} d_j}{D}. \tag{4.30}$$

Auf der anderen Seite gilt aber

$$\sum_{\mathbf{a} \bmod \mathbf{d}} |\mathcal{N}(\mathbf{a})| = \sum_{\mathbf{a} \bmod \mathbf{d}} \sum_{\substack{0 \le n < \prod_{j=1}^{l} d_j \\ (\mathbf{u}n+\mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}}} 1 = \sum_{0 \le n < \prod_{j=1}^{l} d_j} \sum_{\substack{\mathbf{a} \bmod \mathbf{d} \\ (\mathbf{u}n+\mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}}} 1.$$

Da es für jedes n ein eindeutiges Tupel $\mathbf{a} \bmod \mathbf{d}$ gibt, das die Kongruenz $(\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d}$ erfüllt, ist die letzte Doppelsumme gleich $\prod_{j=1}^{l} d_j$. Setzt man dies in die linke Seite von (4.30) ein, so folgt (4.29). □

Damit sind alle Hilfsmittel bereit gestellt, um Satz 4.2 beweisen zu können.

4.3 Der Beweis von Satz 4.2

Beweis von Satz 4.2. Sei $C(N) = |\{0 \le n < N : \mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}\}|$. Es ist zu zeigen, dass $C(N) = \frac{N}{|\mathcal{A}|} + \mathcal{O}\left(N^{1-\delta}\right)$ gilt, falls $\mathbf{a}$ zulässig ist und sonst 0. Man nehme zunächst an, dass $C(N) \neq 0$. Dann existiert eine ganze Zahl n mit $0 \le n < N$, so dass

$$f_j(u_j n + v_j) \equiv a_j \bmod m_j \qquad (1 \le j \le l).$$

Da laut Definition d_j ein Teiler von m_j ist, sind diese Kongruenzen auch mod d_j gültig. Mit Lemma 3.6 folgt $f_j(u_j n + v_j) \equiv (u_j n + v_j)F_j \bmod d_j$ und man erhält insgesamt $(u_j n + v_j)F_j \equiv a_j \bmod d_j$ für $1 \le j \le l$. Damit wäre $\mathbf{a}$ laut Definition zulässig. Also ist $C(N) = 0$, falls $\mathbf{a}$ nicht zulässig ist.

Man nehme nun an, dass $\mathbf{a}$ zulässig ist. Das zu betrachtende Kongruenzsystem $\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}$ ist äquivalent dazu, dass $\mathbf{m} | (\mathbf{f}(\mathbf{u}n + \mathbf{v}) - \mathbf{a})$ komponentenweise

gilt. Nach Lemma 3.4 kann man nun schreiben

$$C(N) = \sum_{n=0}^{N-1} \prod_{j=1}^{l} \left(\frac{1}{m_j} \sum_{h_j=0}^{m_j-1} e\left(\frac{f_j(u_j n + v_j) - a_j}{m_j} h_j \right) \right).$$

Seien

$$\begin{aligned} \mathcal{H} &= \{\mathbf{h} = (h_1, h_2, \ldots, h_l) : 0 \le h_j \le m_j \ (1 \le j \le l)\}, \\ \mathcal{H}_0 &= \{\mathbf{h} = (h_1, h_2, \ldots, h_l) : 0 \le h_j \le m_j \text{ und } m_j | d_j h_j \ (1 \le j \le l)\}. \end{aligned}$$

Umsortieren liefert nun

$$\begin{aligned} C(N) &= \frac{1}{\prod_{j=1}^{l} m_j} \sum_{n=0}^{N-1} \prod_{j=1}^{l} \sum_{h_j=0}^{m_j-1} e\left(\frac{f_j(u_j n + v_j) - a_j}{m_j} h_j \right) \\ &= \frac{1}{\prod_{j=1}^{l} m_j} \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H}} \prod_{j=1}^{l} e\left(\frac{h_j}{m_j} \left(f_j(u_j n + v_j) - a_j \right) \right) \\ &= \frac{1}{\prod_{j=1}^{l} m_j} \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H}} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} \left(f_j(u_j n + v_j) - a_j \right) \right) \\ &= \frac{1}{\prod_{j=1}^{l} m_j} \left(\sum_{1} + \sum_{2} \right), \end{aligned} \tag{4.31}$$

wobei

$$\sum_{1} := \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H}_0} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} \left(f_j(u_j n + v_j) - a_j \right) \right)$$

und

$$\begin{aligned} \sum_{2} :=& \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H} \setminus \mathcal{H}_0} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} \left(f_j(u_j n + v_j) - a_j \right) \right) \\ =& \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H} \setminus \mathcal{H}_0} e\left(\sum_{j=1}^{l} \left(\frac{h_j}{m_j} f_j(u_j n + v_j) - \frac{h_j}{m_j} a_j \right) \right) \\ =& \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H} \setminus \mathcal{H}_0} e\left(\sum_{j=1}^{l} \frac{h_j}{m_j} f_j(u_j n + v_j) \right) e\left(-\sum_{j=1}^{l} \frac{h_j}{m_j} a_j \right) \\ =& \sum_{n=0}^{N-1} \Big(e_1(n, \mathbf{h}_1) e_2(\mathbf{h}_1) + e_1(n, \mathbf{h}_2) e_2(\mathbf{h}_2) + \cdots + e_1(n, \mathbf{h}_k) e_2(\mathbf{h}_k) \Big) \end{aligned}$$

$$
\begin{aligned}
&= e_1(1,\mathbf{h}_1)e_2(\mathbf{h}_1) + e_1(1,\mathbf{h}_2)e_2(\mathbf{h}_2) + \cdots + e_1(1,\mathbf{h}_k)e_2(\mathbf{h}_k) + \cdots + \\
&\quad e_1(N-1,\mathbf{h}_1)e_2(\mathbf{h}_1) + e_1(N-1,\mathbf{h}_2)e_2(\mathbf{h}_2) + \cdots + e_1(N-1,\mathbf{h}_k)e_2(\mathbf{h}_k) \\
&= e_2(\mathbf{h}_1)\sum_{n=0}^{N-1} e_1(n,\mathbf{h}_1) + \cdots + e_2(\mathbf{h}_k)\sum_{n=0}^{N-1} e_1(n,\mathbf{h}_k) \\
&= \sum_{i=1}^{k} e_2(\mathbf{h}_i)\sum_{n=0}^{N-1} e_1(n,\mathbf{h}_i) \\
&= \sum_{\mathbf{h}\in\mathcal{H}\backslash\mathcal{H}_0} e\left(-\sum_{j=1}^{l}\frac{h_j}{m_j}a_j\right)\sum_{n=0}^{N-1} e\left(\sum_{j=1}^{l}\frac{h_j}{m_j}f_j(u_jn+v_j)\right),
\end{aligned}
$$

mit $e_1(n,\mathbf{h}) = e\left(\sum_{j=1}^{l}\frac{h_j}{m_j}f_j(u_jn+v_j)\right)$, $e_2(\mathbf{h}) = e\left(-\sum_{j=1}^{l}\frac{h_j}{m_j}a_j\right)$ und $\mathcal{H}\backslash\mathcal{H}_0 = \{\mathbf{h}_1,\ldots,\mathbf{h}_k\}$. Da $\mathbf{h}\in\mathcal{H}\backslash\mathcal{H}_0$ ist, folgt aus Proposition 4.9

$$
\sum_{n=0}^{N-1} e\left(\sum_{j=1}^{l}\frac{h_j}{m_j}f_j(u_jn+v_j)\right) = \mathcal{O}\left(N^{1-\delta}\right)
$$

mit $\delta = \frac{1}{120l^2\overline{q}^3\overline{m}^2}$. Also ist

$$
\sum_{2} = \mathcal{O}\left(|\mathcal{H}\backslash\mathcal{H}_0|N^{1-\delta}\right) = \mathcal{O}\left(N^{1-\delta}\right). \tag{4.32}
$$

Die Bedingung $m_j|d_jh_j$ ist äquivalent zu $\frac{m_j}{d_j}|h_j$. Setze $h'_j = h_j\frac{d_j}{m_j}$. Somit lässt sich $\mathcal{H}_0$ wie folgt schreiben

$$
\mathcal{H}_0 = \left\{\mathbf{h} = \left(\frac{m_1}{d_1}h'_1, \frac{m_2}{d_2}h'_2, \ldots, \frac{m_l}{d_l}h'_l\right) : 0\le h'_j\le d_j(1\le j\le l)\right\}.
$$

Setze $\mathcal{H}'_0 = \left\{\mathbf{h}' = (h'_1,h'_2,\ldots,h'_l) : 0\le h'_j\le d_j(1\le j\le l)\right\}$. Dann ist

$$
\sum_{\mathbf{h}\in\mathcal{H}_0} e\left(\sum_{j=1}^{l}\frac{h_j}{m_j}\left(f_j(u_jn+v_j)-a_j\right)\right) = \sum_{\mathbf{h}'\in\mathcal{H}'_0} e\left(\sum_{j=1}^{l}\frac{h'_j}{d_j}\left(f_j(u_jn+v_j)-a_j\right)\right).
$$

Laut Lemma 3.6 gilt $f_j(u_jn+v_j)\equiv(u_jn+v_j)F_j \bmod d_j$. Dies und erneutes Umsortieren liefert

$$
\begin{aligned}
\sum_{1} &= \sum_{n=0}^{N-1}\sum_{\mathbf{h}'\in\mathcal{H}'} e\left(\sum_{j=1}^{l}\frac{h'_j}{d_j}\left((u_jn+v_j)F_j-a_j\right)\right) \\
&= \sum_{n=0}^{N-1}\prod_{j=1}^{l}\left(\sum_{h'_j=0}^{d_j-1} e\left(\frac{h'_j}{d_j}\left((u_jn+v_j)F_j-a_j\right)\right)\right) \\
&= \left(\prod_{j=1}^{l}d_j\right)\sum_{n=0}^{N-1}\prod_{j=1}^{l}\left(\frac{1}{d_j}\sum_{h'_j=0}^{d_j-1} e\left(\frac{h'_j}{d_j}\left((u_jn+v_j)F_j-a_j\right)\right)\right).
\end{aligned}
$$

Nach Lemma 3.4 ist die innere Summe gleich d_j, falls $(u_j n + v_j)F_j \equiv a_j \bmod d_j$ ist und 0 andernfalls. Also gilt

$$\sum_1 = \left(\prod_{j=1}^{l} d_j\right) \left|\{0 \le n < N : (u_j n + v_j)F_j \equiv a_j \bmod d_j \quad (1 \le j \le l)\}\right|.$$

Mit (4.28) und (4.29) und der Annahme, dass $\mathbf{a}$ zulässig ist, folgt

$$\begin{aligned}\sum_1 &= \left(\prod_{j=1}^{l} d_j\right)\left(\frac{N}{D} + \mathcal{O}(1)\right) \\ &= \left(\prod_{j=1}^{l} d_j\right)\left(\frac{N}{|\mathcal{A}|}\prod_{j=1}^{l}\frac{m_j}{d_j} + \mathcal{O}(1)\right) \\ &= \frac{N}{|\mathcal{A}|}\prod_{j=1}^{l} m_j + \mathcal{O}(1). \qquad (4.33)\end{aligned}$$

Setzt man nun (4.32) und (4.33) in (4.31) ein, so erhält man

$$C(N) = \frac{N}{|\mathcal{A}|} + \mathcal{O}\left(N^{1-\delta}\right),$$

was zu zeigen war. □

4.4 Folgerungen

Mit Satz 4.2 kann nun das folgende wichtige Resultat geschlossen werden. Es findet direkte Anwendung im zweiten Abschnitt des fünften Kapitels.

Korollar 4.12 *Seien* $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{f}$ *und* δ *wie im ersten Abschnitt des Kapitels bzw. in Satz 4.2 gegeben. Dann gilt*

$$|\{0 \le n < N : \mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}\}| = \frac{N}{m_1 m_2 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right) \qquad (4.34)$$

für alle Tupel $\mathbf{a}$ *genau dann, wenn*

$$(u_j F_j, d_j) = 1 \qquad (1 \le j \le l), \qquad (4.35)$$

$$(d_i, d_j) = 1 \qquad (1 \le i < j \le l). \qquad (4.36)$$

Beweis. Sei zunächst die Gleichung (4.34) für alle $\mathbf{a}$ erfüllt. Damit existiert für alle $\mathbf{a}$ ein n mit $\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{m}$, woraus

$$\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv \mathbf{a} \bmod \mathbf{d}$$

folgt, da $\mathbf{d}|\mathbf{m}$ komponentenweise gilt. Aus Lemma 3.6 folgt

$$\mathbf{f}(\mathbf{u}n + \mathbf{v}) \equiv (\mathbf{u}n + \mathbf{v})\mathbf{F} \bmod \mathbf{d}.$$

Und aus diesen beiden Kongruenzen folgt wiederum

$$(\mathbf{u}n + \mathbf{v})\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d},$$

was laut Definition gleichbedeutend damit ist, dass alle $\mathbf{a}$ zulässig bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u}$, $\mathbf{v}$ und $\mathbf{f}$ sind. Damit ist $|\mathcal{A}| = \prod_{j=1}^{l} m_j$. Insbesondere ist also $(v_1F_1 + 1, \ldots, v_lF_l + 1)$ zulässig, so dass aus Lemma 4.11 (i) $(u_jF_j, d_j) = 1$ folgt. Damit gilt $d_j^* = d_j$ für alle j. Aus Lemma 4.11 (iii) folgt

$$|\mathcal{A}| = \prod_{j=1}^{l} m_j = \left(\prod_{j=1}^{l} \frac{m_j}{d_j}\right) D,$$

woraus direkt folgt, dass $D = kgV\,(d_1^*, \ldots, d_l^*) = kgV\,(d_1, \ldots, d_l) = \prod_{j=1}^{l} d_j$, was impliziert, dass die d_j paarweise teilerfremd sind.

Seien nun die Gleichungen (4.35) und (4.36) erfüllt. Dann gilt wegen (4.35) trivialerweise $(u_jF_j, d_j)|(a_j - v_jF_j)$. Außerdem folgt $(d_i^*, d_j^*) = 1$, womit $a_i^*F_j^* \equiv a_j^*F_i^* \bmod (d_i^*, d_j^*)$ ebenfalls gezeigt ist. Mit Lemma 4.11 (i) folgt dann, dass alle Tupel $\mathbf{a}$ zulässig sind. Die zu beweisende Abschätzung ergibt sich damit direkt aus Satz 4.2. □

Die beiden folgenden Aussagen dienen dazu, das in Satz 4.15 beschriebene Resultat von Berend und Kolesnik [2] mit dem Hauptresultat diese Kapitels, Korollar 4.12, in Beziehung zu setzen.

Satz 4.13 *Gegeben seien die ganzzahligen $2l$-Tupel $\mathbf{q} = (q_1, q_2, \ldots, q_{2l})$ und $\mathbf{m} = (m_1, m_2, \ldots, m_{2l})$ mit $q_j, m_j \geq 2$ für $j = 1, \ldots, 2l$ und $(q_i, q_j) = 1$ für $i \neq j$. Sei $m \in \mathbb{N}_{\geq 2}$. Für jedes j sei f_j eine vollständig q_j-additive Funktion mit ganzzahligen*

Werten, es sei $\mathbf{f} = (f_1, f_2, \ldots, f_{2l})$. *Außerdem sei* $\left(m, q_j^{t_j}\right) = (m, q_j)$ *für* $t_j \geq 2$. *Für beliebige ganzzahlige* $2l$*-Tupel* $\mathbf{a} = (a_1, a_2, \ldots, a_{2l})$, $a, m \in \mathbb{Z}$ *und alle* $N \in \mathbb{N}$ *gilt*

$$|\{0 \leq n < N : n \equiv a \bmod m, \mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}\}| = \begin{cases} \frac{N}{m|\mathcal{A}|} + \mathcal{O}\left(N^{1-\delta}\right) & \textit{falls } \mathbf{a} \textit{ zulässig ist} \\ 0 & \textit{sonst,} \end{cases}$$

wobei $\delta = \frac{1}{480 l^2 \overline{q}^3 \overline{m}^2}$ *ist, mit* $\overline{q} = \max_{1 \leq i \leq 2l} q_i$ *und* $\overline{m} = \max_{1 \leq i \leq 2l} m_i$ *und die Konstante des* $\mathcal{O}$*-Terms nur von* l, m *und* $\mathbf{q}$ *abhängt.*

Beweis. Es gilt

$$\begin{aligned} &|\{0 \leq n < N \ : n \equiv a \bmod m, \ \mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}\}| \\ &\quad = \left| \left\{ 0 \leq \nu < \left[\frac{N}{m}\right] + \kappa : f_1(m\nu + a) \equiv a_1 \bmod m_1, \ldots, \right. \right. \\ &\qquad\qquad \left. \left. f_{2l}(m\nu + a) \equiv a_{2l} \bmod m_{2l} \right\} \right| \\ &\quad = \begin{cases} \frac{\left[\frac{N}{m}\right] + \kappa}{|\mathcal{A}|} + \mathcal{O}\left(\left(\left[\frac{N}{m}\right] + \kappa\right)^{1-\delta}\right) & \text{falls } \mathbf{a} \text{ zulässig ist} \\ 0 & \text{sonst,} \end{cases} \end{aligned}$$

wobei $\kappa \in \{0, 1\}$ in Abhängigkeit von N passend gewählt wird und in der letzten Gleichung Satz 4.2 angewendet wurde. Hieraus folgt direkt die Aussage des Satzes. □

Aus diesem Satz kann man nun wiederum das folgende Korollar schließen.

Korollar 4.14 *Seien* $\mathbf{q}$, $\mathbf{m}$ *und* $\mathbf{f}$ *und* δ *wie in Satz 4.13 gegeben. Für beliebige ganzzahlige* $2l$*-Tupel* $\mathbf{a} = (a_1, a_2, \ldots, a_{2l})$, $a, m \in \mathbb{Z}$ *und alle* $N \in \mathbb{N}$ *gilt*

$$|\{0 \leq n < N : n \equiv a \bmod m, \mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}\}| = \frac{N}{m m_1 m_2 \cdots m_{2l}} + \mathcal{O}\left(N^{1-\delta}\right) \tag{4.37}$$

für alle Tupel $\mathbf{a}$ *genau dann, wenn*

$$(mF_j, d_j) = 1 \qquad (1 \leq j \leq 2l), \tag{4.38}$$

$$(d_i, d_j) = 1 \qquad (1 \leq i < j \leq 2l). \tag{4.39}$$

Beweis. Der Beweis verläuft ganz analog zu dem von Korollar 4.12, wobei Satz 4.13 an Stelle von Satz 4.2 verwendet wird. Sei zunächst die Gleichung (4.37) für alle $\mathbf{a}$ erfüllt. Damit existiert für alle $\mathbf{a}$ ein $0 \leq n < N$ mit $n \equiv a \bmod m$ und $\mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}$. Dies ist gleichbedeutend damit, dass ein ν $(0 \leq \nu < \left[\frac{N}{m}\right])$ existiert mit

$$\mathbf{f}(m\nu + a) \equiv \mathbf{a} \bmod \mathbf{m},$$

woraus

$$\mathbf{f}(m\nu + a) \equiv \mathbf{a} \bmod \mathbf{d}$$

folgt, da $\mathbf{d}|\mathbf{m}$ komponentenweise gilt. Aus Lemma 3.6 folgt

$$\mathbf{f}(m\nu + a) \equiv (m\nu + a)\mathbf{F} \bmod \mathbf{d}.$$

Und aus diesen beiden Kongruenzen folgt wiederum

$$(m\nu + a)\mathbf{F} \equiv \mathbf{a} \bmod \mathbf{d},$$

was laut Definition gleichbedeutend damit ist, dass alle $\mathbf{a}$ zulässig bezüglich $\mathbf{q}$, $\mathbf{m}$, $\mathbf{u} = (m, \ldots, m)$, $\mathbf{v} = (a, \ldots, a)$ und $\mathbf{f}$ sind. Damit ist $|\mathcal{A}| = \prod_{j=1}^{2l} m_j$. Insbesondere ist also $(aF_1 + 1, \ldots, aF_{2l} + 1)$ zulässig, so dass aus Lemma 4.11 (i) $(mF_j, d_j)|1$ folgt. Damit gilt $d_j^* = d_j$ für alle j. Aus Lemma 4.11 (iii) folgt

$$|\mathcal{A}| = \prod_{j=1}^{2l} m_j = \left(\prod_{j=1}^{2l} \frac{m_j}{d_j}\right) D,$$

woraus direkt folgt, dass $D = kgV\left(d_1^*, \ldots, d_{2l}^*\right) = kgV\left(d_1, \ldots, d_{2l}\right) = \prod_{j=1}^{2l} d_j$, was impliziert, dass die d_j paarweise teilerfremd sind.

Seien nun die Gleichungen (4.38) und (4.39) erfüllt. Dann gilt wegen (4.37) trivialerweise die Teilbarkeitseigenschaft $(mF_j, d_j)|(a_j - aF_j)$. Außerdem folgt $(d_i^*, d_j^*) = 1$, womit $a_i^* F_j^* \equiv a_j^* F_i^* \bmod (d_i^*, d_j^*)$ gezeigt ist. Mit Lemma 4.11 (i) folgt dann, dass alle Tupel $\mathbf{a}$ zulässig sind. Die zu beweisende Abschätzung ergibt sich damit direkt aus Satz 4.13. □

Der folgende Satz entstammt einem Artikel von Berend und Kolesnik [2]. Diese folgten ebenfalls der Idee von Luca und Stănică und modifizierten den Satz von Kim, jedoch nicht in der Allgemeinheit, wie es in [16] angedacht wurde. Ihr Resultat lautet wie folgt.

Satz 4.15 [2, Theorem 2.6] *Seien $q_1, \ldots, q_l \geq 3$ paarweise verschiedene ganze Zahlen. Für jedes $1 \leq j \leq l$ seien f_j und f_{l+j} vollständig q_j-additive Funktionen mit ganzzahligen Werten und $\mathbf{f} = (f_1, \ldots, f_{2l})$. Seien m_j und m_{l+j} $(1 \leq j \leq l)$ teilerfremde positive ganze Zahlen mit*

$$\begin{aligned} \mathrm{ggT}\{m_j, f_j(r) - rF_j \ (2 \leq r \leq q_j - 1)\} &= 1, \qquad (4.40) \\ \mathrm{ggT}\{m_{l+j}, f_{l+j}(r) - rF_j \ (2 \leq r \leq q_j - 1)\} &= 1 \qquad (4.41) \end{aligned}$$

und $\mathbf{m} = (m_1, \ldots, m_{2l})$. Sei $M = max_{1 \leq j \leq l} m_j m_{l+j}$ und $\mathbf{a} = (a_1, a_2, \ldots, a_{2l})$ ein $2l$-Tupel mit ganzzahligen Einträgen. Dann gilt für ganze Zahlen $m \geq 2$ und a

$$\begin{aligned} &|\{0 \leq n < N : n \equiv a \bmod m, \ \mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}\}| \\ &\qquad = \frac{N}{m m_1 \cdots m_{2l}} + \mathcal{O}\left(N^{1-\delta}\right), \qquad (4.42) \end{aligned}$$

wobei $\delta = \frac{4}{\overline{q}^2 M^2 l \log \overline{q} + 8l + 8}$ ist.

Bemerkung 4.16 Vergleicht man nun Korollar 4.14 mit Satz 4.15, so stellt man fest, dass Korollar 4.14 mit der Bedingung $(q_i, q_j) = 1$ für $1 \leq i < j \leq 2l$ eine stärkere Anforderung an die q_i stellt als Satz 4.15. Würde man dies auch in Satz 4.15 fordern, so wären aber mit den Gleichungen (4.40) und (4.41) insbesondere die Gleichungen (4.38) und (4.39) erfüllt. Außerdem wird in Korollar 4.14 zusätzlich vorausgesetzt, dass $\left(m, q_j^{t_j}\right) = (m, q_j)$ für $t_j \geq 2$ gilt. Diese Voraussetzung stammt aus dem Satz 4.2, in dem gefordert wurde, dass $\left(u_j, q_j^{t_j}\right) = (u_j, q_j)$ für $t_j \geq 2$ gilt. Diese Bedingung ist hier notwendig, da sich, wie in Lemma 4.5 geschehen, $\Phi^*_{qN}(qk + r)$ sonst nicht in Abhängigkeit von $\Phi_N(k)$ und $\Phi_N(k+1)$ darstellen lässt und somit der Satz mit den Mittel von Kim nicht mehr zu beweisen ist. Es ist nicht klar, ob der Satz 4.2 ohne die genannte Bedingung gilt. Ein dritter Unterschied liegt im Fehlerterm. Berend und Kolesnik [2] erhalten einen etwas besseren Fehlerterm, da sie in ihrem Beweis schon frühzeitig die Voraussetzungen, die sie an $\mathbf{q}$, $\mathbf{m}$ und $\mathbf{f}$ stellen, ausnutzen.

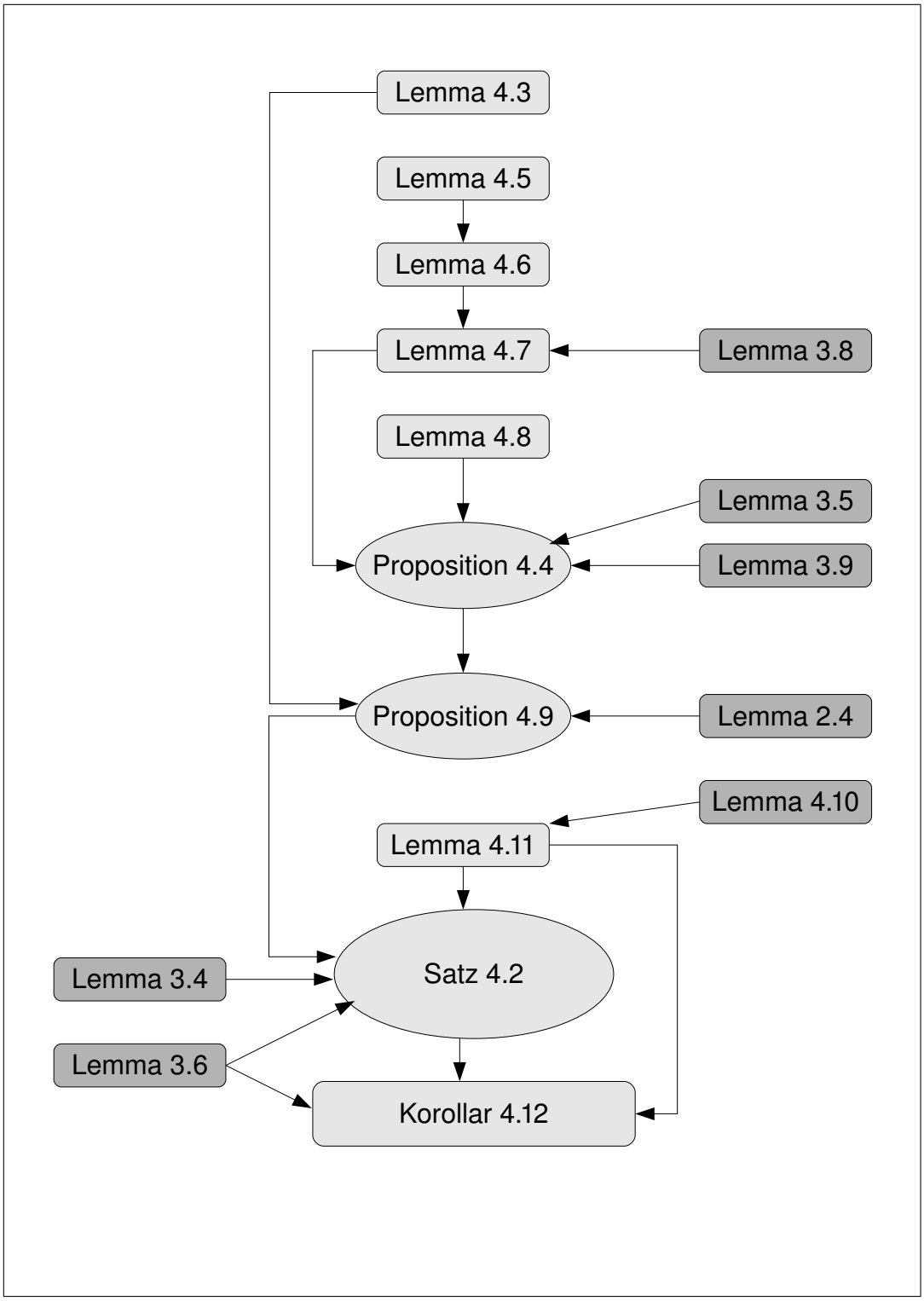

Abbildung 4.1: Übersicht über die Beweiskette

Kapitel 5

Die Primfaktorzerlegung von n!

In diesem Kapitel wird zunächst ein Satz von Luca und Stănică [16] vorgestellt sowie dessen Beweis näher erläutert. Diese konstruierten eine vollständig q_i-additive Funktion, die kongruent zu $e_{p_i}(n!)$ ist und auf welche sich der Satz von Kim, Satz 3.2, anwenden lässt. Da bei der Konstruktion der kleine Satz von Fermat verwendet wird, welcher voraussetzt, dass $p_i \nmid m_i$ gilt, können Luca und Stănică mit der Verwendung von Satz 3.2 auch nur für diesen Fall die Gleichverteilung der Exponenten in der Primfaktorzerlegung von $n!$ zeigen.

Gemäß der Idee von Luca und Stănică, den Satz von Kim zu verallgemeinern, wie es im vierten Kapitel durchgeführt wurde, wird daraufhin im zweiten Abschnitt die Ziffernsumme sowie Korollar 4.12 verwendet, um den Fall $m_i = p_i$ bzw. $m_i = p_i^{\alpha_i}$ mit $\alpha_i \geq 1$ zu beweisen. Die Ergebnisse sind schrittweise in den Sätzen 5.3, 5.5 und 5.6 sowie in Bemerkung 5.7 formuliert. Das erwünschte Resultat, dass neben den m_i, die nicht von p_i geteilt werden, auch Einträge in $\mathbf{m}$ enthalten sein dürfen, die Potenzen der jeweiligen Primzahlen sind, könnte auch zu einem Satz zusammen gefasst werden. Hierauf wurde aber zu Gunsten der besseren Verständlichkeit verzichtet.

Im allgemeinen Fall eignet sich die Ziffernsumme jedoch nicht für einen Beweis, da sich die Kongruenz zu $e_{p_i}(n!)$ modulo m_i im Allgemeinen nicht geeignet formulieren lässt. Um diese Problem zu umgehen spalten Berend und Kolesnik [2] die Kongruenzen modulo m_i in zwei Kongruenzen modulo k_i und modulo $p_i^{\alpha_i}$ auf. Auf diese wenden sie ihre Modifikation des Satzes von Kim, Satz 4.15, an. Dieses Vorgehen wird im dritten

Abschnitt des Kapitel erläutert. Jedoch geht aus dem Beweis nicht hervor, wie die Aussage für den Fall $\alpha_i = 1$ geschlossen wird, weshalb dieser Fall in der Formulierung von Satz 5.9 ausgeschlossen wird.

Abschließend wird im vierten Abschnitt des Kapitels der Fehlerterm betrachtet. Wie anhand der Beispiele zu sehen ist, kann zwar der Fehler auch deutlich geringer ausfallen als $\mathcal{O}\left(N^{1-\delta}\right)$, jedoch ist dies nicht die Regel, so dass der Fehlerterm, der in den vorigen Abschnitten erhalten wird, nicht deutlich verbessert werden kann.

5.1 Der Fall $\mathbf{p_i \nmid m_i}$

Satz 5.1 [16, Theorem 1] *Seien $p_1, \ldots, p_l$ verschiedene Primzahlen, $m_1, \ldots, m_l$ beliebige positive ganze Zahlen mit $m_i \geq 2$ $(i = 1, \ldots, l)$ und $0 \leq a_i \leq m_i - 1$ $(i = 1, \ldots, l)$ beliebige Restklassen modulo m_i. Außerdem wird angenommen, dass $p_i \nmid m_i$ für alle $i = 1, \ldots, l$ gilt. Dann gilt*

$$|\{0 \leq n < N : e_{p_i}(n!) \equiv a_i \mod m_i,\ 1 \leq i \leq l\}| = \frac{N}{m_1 \cdots m_l} + O\left(N^{1-\delta}\right)$$

mit $\delta = \frac{1}{120 l^2 \overline{p}^{3\overline{m}} \overline{m}^2}$, wobei $\overline{p} = \max_{1 \leq i \leq l} p_i$ und $\overline{m} = \max_{1 \leq i \leq l} m_i$ sind.

Beweis. Für einen festen Index i sei λ_i eine minimale positive ganze Zahl, so dass die Kongruenz $\frac{p_i^{\lambda_i} - 1}{p_i - 1} \equiv 0 \mod m_i$ erfüllt ist. Zunächst wird die Existenz dieser Zahl gezeigt. Laut dem kleinen Satz von Fermat gilt $p_i^{\varphi(m_i)} - 1 \equiv 0 \mod m_i$, falls $(p_i, m_i) = 1$, was gleichbedeutend mit $p_i \nmid m_i$ ist, was wiederum in diesem Satz vorausgesetzt wird. Diese Kongruenz ist äquivalent zu $\frac{p_i^{\varphi(m_i)} - 1}{p_i - 1} \equiv 0 \mod \frac{m_i}{(p_i - 1, m_i)}$, woraus $\frac{p_i^{\varphi(m_i)} - 1}{p_i - 1} \equiv 0 \mod m_i$ für den Fall $(p_i - 1, m_i) = 1$ folgt. φ sei hier die Eulersche φ-Funktion. Im Fall $(p_i - 1, m_i) > 1$ wähle man ein geeignetes x, so dass $m_i = \frac{x}{(p_i - 1, x)}$ mit $(p_i, x) = 1$. Dann gilt also $\frac{p_i^{\varphi(x)} - 1}{p_i - 1} \equiv 0 \mod \frac{x}{(p_i - 1, x)}$ und damit $\frac{p_i^{\varphi(x)} - 1}{p_i - 1} \equiv 0 \mod m_i$. Dies leistet zum Beispiel $x = (p_i - 1) m_i$.

Offensichtlich ist $\lambda_i \geq 2$, da $m_i \geq 2$ und die Kongruenz somit für $\lambda_i = 1$ nicht gilt. Um nun λ_i abzuschätzen, schreibe man $m_i = m_i' m_i''$, wobei m_i' und m_i'' teilerfremd sind, all die Primfaktoren von m_i' den Term $p_i - 1$ teilen und m_i'' teilerfremd zu $p_i - 1$ ist. Es ist offensichtlich, dass m_i' und m_i'' eindeutig bestimmt sind.

Dann erfüllt die Zahl $\mu_i = m_i' \varphi(m_i'')$ die Bedingung $\frac{p_i^{\mu_i}-1}{p_i-1} \equiv 0 \mod m_i$, denn diese Kongruenz ist äquivalent dazu, dass die beiden Äquivalenzen $\frac{p_i^{\mu_i}-1}{p_i-1} \equiv 0 \mod m_i'$ und $\frac{p_i^{\mu_i}-1}{p_i-1} \equiv 0 \mod m_i''$ gelten. Da m_i'' teilerfremd zu $p_i - 1$ ist, ist $\frac{p_i^{\mu_i}-1}{p_i-1} \equiv 0 \mod m_i''$ wiederum äquivalent zu $p_i^{\mu_i} - 1 \equiv 0 \mod m_i''$. Nun gilt nach dem kleinen Satz von Fermat

$$p_i^{\mu_i} - 1 = \left(p_i^{\varphi(m_i'')}\right)^{m_i'} - 1 \equiv 1 - 1 \mod m_i'',$$

womit die zweite Kongruenz gezeigt ist. Aus $m_i' | (p_i - 1)$ folgt, dass $p_i \equiv 1 \mod m_i'$ ist. Damit gilt

$$\begin{aligned} \frac{p_i^{m_i'\varphi(m_i'')} - 1}{p_i - 1} &= p_i^{m_i'\varphi(m_i'')-1} + \cdots + p_i^{m_i'} + p_i^{m_i'-1} + \cdots + p_i + 1 \\ &\equiv m_i'\varphi(m_i'') \mod m_i' \\ &\equiv 0 \mod m_i'. \end{aligned}$$

Falls $m_i = 2$ ist, so ist $p_i \neq 2$ und somit ist dann $\lambda_i = m_i' = m_i = 2$. Falls $m_i > 2$ ist, so ist entweder $m_i' \geq 2$ oder $\varphi(m_i'') = \varphi(m_i) \geq 2$. Insbesondere ist $\lambda_i \leq m_i \leq \overline{m}$.

Setze nun $q_i = p_i^{\lambda_i}$. Man beachte, dass $(q_i, q_j) = 1$ für $i \neq j$ und $\overline{q} = \max_{1 \leq i \leq l} q_i \leq \overline{p}^{\overline{m}}$ gilt. Definiere die vollständig q_i-additive Funktion f_i wie folgt. Sei a eine ganze Zahl mit $0 \leq a \leq q_i - 1$ und mit p_i-adischer Entwicklung

$$a = a_0 + a_1 p_i + a_2 p_i^2 + \cdots + a_{\lambda_i - 1} p_i^{\lambda_i - 1} \tag{5.1}$$

mit $0 \leq a_j \leq p_i - 1$ für $j = 0, 1, \ldots, \lambda_i - 1$. Setze

$$f_i(a) = a_0 \frac{p_i^0 - 1}{p_i - 1} + a_1 \frac{p_i - 1}{p_i - 1} + \cdots + a_{\lambda_i - 1} \frac{p_i^{\lambda_i - 1} - 1}{p_i - 1} \tag{5.2}$$

und setze die Funktion f_i auf allen nicht negativen ganzen Zahlen fort, so dass sie vollständig q_i-additiv ist. Dies erhält man wie folgt. Sei $n \geq 0$ und schreibe

$$n = n_0 + n_1 p_i + n_2 p_i^2 + \cdots + n_t p_i^t \tag{5.3}$$

mit $0 \leq n_j \leq p_i - 1$ für $j = 0, 1, \ldots, t$. Nun sei für alle nicht negativen ganzen Zahlen j die Zahl $\overline{j}$ mit $\overline{j} \equiv j \mod \lambda_j$ der kleinste Rest modulo λ_j. Dann sei

$$f_i(n) = \sum_{j=0}^{t} n_j \frac{p_i^{\overline{j}} - 1}{p_i - 1}. \tag{5.4}$$

Als nächstes ist zu zeigen, dass $f_i(n) \equiv e_{p_i}(n!) \mod m_i$ ist. Hierfür wird zunächst induktiv gezeigt, dass $e_{p_i}(n!) = \frac{n-S_{p_i}(n)}{p_i-1}$ gilt, wobei $S_{p_i}(n)$ die Ziffernsumme der p_i-adischen Entwicklung von n sei.

Ist $n = 1$, so gilt $e_{p_i}(n!) = 0$ für alle p_i und $\frac{n-S_{p_i}(n)}{p_i-1} = \frac{1-1}{p_i-1} = 0$. Man nehme an, dass die Behauptung für n gilt. Sei $k \geq 0$ der kleinste Index mit $n_k \neq p_i - 1$. Im Fall $n_0 = \cdots = n_t$ ist $k = t + 1$, da $n_{t+1} = 0$ ist. Dann gilt

$$\begin{aligned} n+1 &= 1 + (p_i - 1) + (p_i - 1)p_i + \cdots + (p_i - 1)p_i^{k-1} + n_k p_i^k + \cdots + n_t p^t \\ &= (n_k + 1)p_i^k + \cdots + n_t p_i^t \\ &= p_i^k \left((n_k + 1) + n_{k+1} p_i + \cdots + n_t p_i^{t-k} \right). \end{aligned} \tag{5.5}$$

Hieran kann man ablesen, dass $e_{p_i}(n + 1) = k$ ist. Zusammen mit der Induktionsvermutung folgt daraus

$$\begin{aligned} e_{p_i}((n+1)!) &= e_{p_i}(n!(n+1)) = e_{p_i}(n!) + e_{p_i}((n+1)) \\ &= \frac{n - S_{p_i}(n)}{p_i - 1} + k \\ &= \frac{n - S_{p_i}(n) + k(p_i - 1)}{p_i - 1} \\ &= \frac{(n+1) - (S_{p_i}(n) + 1 - k(p_i - 1))}{p_i - 1}. \end{aligned}$$

Für die Ziffernsumme von $n + 1$ gilt laut (5.5)

$$S_{p_i}(n + 1) = (n_k + 1) + n_{k+1} + \cdots + n_t,$$

für die Ziffernsumme von n gilt

$$S_{p_i}(n) = k(p_i - 1) + n_k + n_{k+1} + \cdots + n_t$$

und damit

$$S_{p_i}(n + 1) = S_{p_i}(n) + 1 - k(p_i - 1),$$

womit die Behauptung für $n + 1$ folgt.

Somit gilt

$$\begin{aligned} e_{p_i}(n!) &= \frac{n - S_{p_i}(n)}{p_i - 1} \\ &= \frac{1}{p_i - 1} \left(\sum_{k=0}^{s} n_k p_i^k - \sum_{k=0}^{s} n_k \right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{s} n_k \frac{p_i^k - 1}{p_i - 1} && (5.6)\\
&= \sum_{k=1}^{s} n_k \left(p_i^{k-1} + p_i^{k-2} + \cdots + p_i + 1\right)\\
&= \sum_{k=1}^{s} \left(n_k p_i^{k-1} + n_k p_i^{k-2} + \cdots + n_k p_i + n_k\right) && (5.7)\\
&\equiv \sum_{k=1}^{s} n_k \mod p_i\\
&\equiv S_{p_i}(n) - n_0 \mod p_i && (5.8)
\end{aligned}
$$

für eine geeignete nicht negative ganze Zahl s. Vergleicht man (5.4) mit (5.6), so folgt, dass es genügt, die Kongruenz

$$\frac{p_i^k - 1}{p_i - 1} \equiv \frac{p_i^{\overline{k}} - 1}{p_i - 1} \mod m_i$$

zu zeigen. Es gilt

$$
\begin{aligned}
& \tfrac{p_i^k - 1}{p_i - 1} \equiv \tfrac{p_i^{\overline{k}} - 1}{p_i - 1} && \mod m_i\\
\Leftrightarrow\ & \tfrac{p_i^k - p_i^{\overline{k}}}{p_i - 1} \equiv 0 && \mod m_i\\
\Leftrightarrow\ & \tfrac{p_i^{\overline{k}}(p_i^{k-\overline{k}} - 1)}{p_i - 1} \equiv 0 && \mod m_i\\
\Leftrightarrow\ & \tfrac{p_i^{k-\overline{k}} - 1}{p_i - 1} \equiv 0 && \mod m_i,
\end{aligned}
$$

da p_i und m_i teilerfremd sind. Die letzte Kongruenz gilt, da $\left(k - \overline{k}\right)$ ein Vielfaches von λ_i ist.

Um nun Korollar 3.3 anwenden zu können, prüfe man, ob $(F_j, d_j) = 1$ für $1 \leq j \leq l$ und $(d_i, d_j) = 1$ für $1 \leq i < j \leq l$ gilt. Wähle $r = p_i$. Dies ist möglich, da $\lambda_i \geq 2$ ist und somit $p_i \leq q_i - 1$. Dann gilt

$$f_i(r) - rF_i = f_i(p_i) - p_i F_i = f_i(p_i) - p_i f_i(1) = f_i(p_i) = 1,$$

laut Definition von F_i und da $f_i(1) = 0$ ist. Somit ist $d_i = 1$ für $1 \leq i \leq l$ und die beiden genannten Bedingungen sind erfüllt. Damit folgt die Behauptung mit Korollar 3.3. □

5.2 Der Fall $\mathbf{m_i = p_i^{\alpha_i}}$ mit $\alpha_\mathbf{i} \geq \mathbf{1}$

Das folgende Lemma dient der Vorbereitung für den Beweis von Satz 5.3.

Lemma 5.2 *Seien $N \equiv t \mod m$ mit $N, m \in \mathbb{N}$, $t \in \mathbb{N}_0$ und $0 \leq t \leq m$. Dann gilt*

$$\sum_{r=0}^{m-1} \left(\left[\frac{N}{m} \right] + \kappa_r \right) = N$$

und

$$0 \leq m\nu + r < N \qquad \text{für } 0 \leq \nu < \left[\frac{N}{m} \right] + \kappa_r \quad \text{und} \quad 0 \leq r < m,$$

wobei $\kappa_r = \begin{cases} 1 & \text{für } 0 \leq r < t \\ 0 & \text{für } t \leq r < m \end{cases}$ *sei.*

Beweis. Laut Definition von κ_r und da $N \equiv t \mod m$ ist, gilt

$$\begin{aligned} \sum_{r=0}^{m-1} \left(\left[\frac{N}{m} \right] + \kappa_r \right) &= \sum_{r=0}^{t-1} \left(\left[\frac{N}{m} \right] + 1 \right) + \sum_{r=t}^{m-1} \left[\frac{N}{m} \right] \\ &= \sum_{r=0}^{m-1} \left[\frac{N}{m} \right] + \sum_{r=0}^{t-1} 1 = \sum_{r=0}^{m-1} \left[\frac{N}{m} \right] + t \\ &= m \left[\frac{N}{m} \right] + t = m \frac{N-t}{m} + t = N. \end{aligned}$$

Nun ist also noch die zweite Behauptung zu zeigen. Sei zunächst $0 \leq r < t$ und $0 \leq \nu \leq \left[\frac{N}{m} \right] + \kappa_r - 1$. Dann gilt

$$m\nu + r \leq m \left(\left[\frac{N}{m} \right] + \kappa_r - 1 \right) + r = m \left[\frac{N}{m} \right] + r = N - t + r < N.$$

Im Fall $t \leq r < m$ und $0 \leq \nu \leq \left[\frac{N}{m} \right] + \kappa_r - 1$ gilt

$$m\nu + r \leq m \left(\left[\frac{N}{m} \right] + \kappa_r - 1 \right) + r = m \left[\frac{N}{m} \right] - m + r = N - t - m + r < N.$$

□

Zunächst wird nun der Fall betrachtet, in dem $m_i = p_j$ für $1 \leq i \leq l$ und $j \in \{1, \ldots, l\}$ gilt.

Satz 5.3 *Seien $p_1, \ldots, p_l$ verschiedene Primzahlen und $\varepsilon_1, \ldots, \varepsilon_l \in \{0, 1, \ldots, p_j - 1\}$ für ein $j \in \{1, \ldots, l\}$. Dann gilt*

$$|\{0 \leq n < N : e_{p_i}(n!) \equiv \varepsilon_i \mod p_j,\ 1 \leq i \leq l\}| = \frac{N}{p_j^l} + \mathcal{O}\left(N^{1-\delta}\right)$$

mit $\delta = \frac{1}{120 l^2 \overline{p}^{3p_j} p_j^2}$, wobei $\overline{p} = \max_{1 \leq i \leq l} p_i$ sei.

Beweis. Definiere für $i = 1, \ldots, l$ mit $i \neq j$ die Funktionen f_i wie im Beweis von Satz 5.1. Dann gilt wiederum $f_i(n) \equiv e_{p_j}(n!)$ für $i = 1, \ldots, l$ mit $i \neq j$. Definiere $f_j(n) = S_{p_j}(n)$, wobei $S_{p_j}(n)$ die Ziffernsumme der p_j-adischen Entwicklung von n bezeichne. Mit (5.8) gilt

$$e_{p_j}(n!) \equiv S_{p_j}(n) - n_0 \mod p_j.$$

Mit dieser Definition von $\mathbf{f}$ betrachte man nun also das Kongruenzsystem

$$f_i(n) \equiv \begin{cases} \varepsilon_i \mod p_j & \text{für } i = 1, \ldots, l \text{ mit } i \neq j \\ \varepsilon_i + n_0 \mod p_j & \text{sonst,} \end{cases}$$

wobei $n_0 = 0$ ist, falls $p_j | n$. Man setze $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{j-1}, \varepsilon_j + n_0, \varepsilon_{j+1}, \ldots, \varepsilon_l)$, wobei die j-te Komponente mod p_j betrachtet wird. Damit ist

$$|\{0 \leq n < N : \mathbf{f}(n) \equiv \varepsilon \mod p_j\}|$$

abzuschätzen. Der Satz von Kim, Satz 3.2, kann hier nicht angewendet werden, da ε nicht fest ist. Aus diesem Grund betrachte man nun die Fälle $n \equiv 0 \mod p_j, n \equiv 1 \mod p_j, \ldots, n \equiv p_j - 1 \mod p_j$ einzeln. Dann gilt mit Korollar 4.12 und Lemma 5.2

$$\begin{aligned} &|\{0 \leq n < N : e_{p_i}(n!) \equiv \varepsilon_i \mod p_j,\ 1 \leq i \leq l\}| \\ &\quad = |\{0 \leq n < N : \mathbf{f}(n) \equiv \varepsilon \mod p_j\}| \\ &\quad = \left|\left\{0 \leq \nu < \left[\frac{N}{p_j}\right] + \kappa_0 : \mathbf{f}(p_j\nu) \equiv \varepsilon \mod p_j\right\}\right| \\ &\qquad + \left|\left\{0 \leq \nu < \left[\frac{N}{p_j}\right] + \kappa_1 : \mathbf{f}(p_j\nu + 1) \equiv \varepsilon \mod p_j\right\}\right| \\ &\qquad + \cdots + \left|\left\{0 \leq \nu < \left[\frac{N}{p_j}\right] + \kappa_{p_j - 1} : \mathbf{f}(p_j\nu + p_j - 1) \equiv \varepsilon \mod p_j\right\}\right| \end{aligned}$$

$$
\begin{aligned}
&= \frac{\left[\frac{N}{p_j}\right] + \kappa_0}{p_j^l} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_0\right)^{1-\delta}\right) \\
&\quad + \frac{\left[\frac{N}{p_j}\right] + \kappa_1}{p_j^l} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_1\right)^{1-\delta}\right) \\
&\quad + \cdots + \frac{\left[\frac{N}{p_j}\right] + \kappa_{p_j-1}}{p_j^l} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_{p_j-1}\right)^{1-\delta}\right) \\
&= \frac{N}{p_j^l} + \mathcal{O}\left(N^{1-\delta}\right),
\end{aligned}
$$

wobei noch zu prüfen ist, ob die Voraussetzungen von Korollar 4.12 erfüllt sind.

Mit $q_i = p_i^{\lambda_i}$ für $i = 1, \ldots, l$ und $i \neq j$ und $q_j = p_j$ ist f_i für alle i vollständig q_i-additiv. Es gilt $\mathbf{u} = (p_j, \ldots, p_j)$, $F_j = f_j(1) = 1$ und $F_i = f_i(1) = 0$ für $i = 1, \ldots, l$ und $i \neq j$ und $d_j = (p_j, p_j - 1) = 1$. Wähle $r = p_i$ für $i \neq j$. Dann gilt erneut $f_i(r) - rF_i = 1$ für $i \neq j$. Damit ist also auch für $i \neq j$ $d_i = 1$ und die Voraussetzungen von Korollar 4.12 sind erfüllt. Außerdem gilt für alle i und $t_i \geq 2$ $\left(u_i, q_i^{t_i}\right) = \left(p_j, q_i^{t_i}\right) = (p_i, q_i) = (u_i, q_i)$, da es sich bei q_i um Primzahlpotenzen handelt. Damit folgt der Satz. □

Bemerkung 5.4 Mit $p = 2$ entspricht Satz 5.3 einer Vermutung von Sander [18], welche somit bewiesen ist.

Nun wird der Fall betrachtet, in dem einige m_i Primzahlen sind, für die übrigen aber $p_i \nmid m_i$ gilt.

Satz 5.5 *Seien $p_1, p_2, \ldots, p_l$ verschiedene Primzahlen, $m_1, m_2, \ldots, m_l$ beliebige positive ganze Zahlen mit $m_i \geq 2$ für $i = 1, \ldots, l$ und $0 \leq a_i \leq m_i - 1$ für $i = 1, \ldots, l$ beliebige Restklassen modulo m_i. Für $j_\mu \in \{1, \ldots, l\}$, $\mu = 1, \ldots, M$ gelte $m_{j_\mu} = p_{j_\mu}$. Außerdem wird angenommen, dass $p_i \nmid m_i$ für $i = 1, \ldots, l$ mit $i \neq j_\mu$. Dann gilt*

$$
\left|\{0 \leq n < N : e_{p_i}(n!) \equiv a_i \mod m_i,\ 1 \leq i \leq l\}\right| = \frac{N}{m_1 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right)
$$

mit $\delta = \frac{1}{120 l^2 \overline{p}^{3\overline{m}} \overline{m}^2}$, wobei $\overline{p} = \max_{1 \leq i \leq l} p_i$ und $\overline{m} = \max_{1 \leq i \leq l} m_i$ sind.

Beweis. Für $i = 1, \ldots, l$, $i \neq j_\mu$ seien die Funktionen f_i wie im Beweis zu Satz 5.1 definiert. Dann gilt wiederum $f_i(n) \equiv e_{p_i}(n!) \bmod m_i$, $i \neq j_\mu$. Definiere $f_{j_\mu}(n) = S_{p_{j_\mu}}(n)$. Laut (5.8) gilt

$$e_{j_\mu}(n!) \equiv S_{p_{j_\mu}}(n) - n_0 \mod p_{j_\mu},$$

was äquivalent ist zu

$$S_{j_\mu}(n) \equiv e_{p_{j_\mu}}(n!) + n_0 \mod p_{j_\mu}.$$

Mit dieser Definition von $\mathbf{f}$ kann man nun das Kongruenzsystem

$$f_i(n) \equiv a_i \mod m_i \text{ für } i = 1, \ldots, l \text{ und } i \neq j_\mu$$

und

$$f_{j_\mu}(n) \equiv \begin{cases} a_{j_\mu} + 0 & \mod p_{j_\mu} \quad \text{falls } n \equiv 0 \mod p_{j_\mu} \\ a_{j_\mu} + 1 & \mod p_{j_\mu} \quad \text{falls } n \equiv 1 \mod p_{j_\mu} \\ \vdots & \\ a_{j_\mu} + (p_{j_\mu} - 1) & \mod p_{j_\mu} \quad \text{falls } n \equiv p_{j_\mu} - 1 \mod p_{j_\mu} \end{cases}$$

betrachten. Nun wende man wiederum das Korollar 4.12 an. Sei $\mathbf{a}^* = (a_1^*, \ldots, a_l^*)$ mit

$$a_i^* = \begin{cases} a_i & \text{falls } i \neq j_\mu \\ a_i + n_0 & \text{falls } i = j_\mu \end{cases}.$$

Da hier wiederum $\mathbf{a}^*$ nicht fest ist, müssen sämtliche Fälle bezüglich der Kongruenz von n modulo der Primzahlen $p_{j_1}, \ldots, p_{j_M}$ unterschieden werden. Man setze hierfür $p = p_{j_1} \cdots p_{j_M}$. Dann gilt

$$\begin{aligned} &|\{0 \leq n < N : \ e_{p_i}(n!) \equiv a_i \bmod m_i \ (1 \leq i \leq l)\}| \\ &\quad = |\{0 \leq n < N : \mathbf{f}(n) \equiv \mathbf{a} \bmod \mathbf{m}\}| \\ &\quad = \left|\left\{0 \leq \nu < \left[\frac{N}{p}\right] + \kappa_0 : \mathbf{f}(p\nu) \equiv \mathbf{a}^* \bmod \mathbf{m}\right\}\right| \\ &\qquad + \left|\left\{0 \leq \nu < \left[\frac{N}{p}\right] + \kappa_1 : \mathbf{f}(p\nu + 1) \equiv \mathbf{a}^* \bmod \mathbf{m}\right\}\right| \\ &\qquad + \cdots + \left|\left\{0 \leq \nu < \left[\frac{N}{p}\right] + \kappa_{p_j - 1} : \mathbf{f}(p\nu + p - 1) \equiv \mathbf{a}^* \bmod \mathbf{m}\right\}\right| \end{aligned}$$

$$
\begin{aligned}
=&\frac{\left[\frac{N}{p}\right]+\kappa_0}{m_1\cdots m_l}+\mathcal{O}\left(\left(\left[\frac{N}{p}\right]+\kappa_0\right)^{1-\delta}\right)\\
&+\frac{\left[\frac{N}{p}\right]+\kappa_1}{m_1\cdots m_l}+\mathcal{O}\left(\left(\left[\frac{N}{p}\right]+\kappa_1\right)^{1-\delta}\right)\\
&+\cdots+\frac{\left[\frac{N}{p}\right]+\kappa_{p_j-1}}{m_1\cdots m_l}+\mathcal{O}\left(\left(\left[\frac{N}{p}\right]+\kappa_{p_j-1}\right)^{1-\delta}\right)\\
=&\frac{N}{m_1\cdots m_l}+\mathcal{O}\left(N^{1-\delta}\right).
\end{aligned}
$$

Es ist noch zu prüfen, ob die Voraussetzungen von Korollar 4.12 erfüllt sind. Setze $q_i = p_i^{\lambda_i}$ für $i \neq j_\mu$ und $q_{j_\mu} = p_{j_\mu}$ für $\mu = 1, \ldots, M$. Es gilt

$$d_{j_\mu} = (m_{j_\mu}, (p_{j_\mu} - 1)F_{j_\mu}) = (p_{j_\mu}, p_{j_\mu} - 1) = 1,$$

da $f_{j_\mu}(r) - rF_{j_\mu} = f_{j_\mu}(r) - r \cdot 1 = r - r = 0$ für $2 \leq r \leq q_{j_\mu} - 1$. Es gilt $d_i = 1$ für $i \neq j_\mu$ und somit $(d_i, d_j) = 1$ für $1 \leq i < j \leq l$. Da $d_j = 1$ für $1 \leq j \leq l$ gilt, ist $(u_j F_j, d_j) = 1$ für $1 \leq j \leq l$. Da die p_i $(1 \leq i \leq l)$ paarweise verschieden sind, gilt $(p_{j_1} \cdots p_{j_M}, q_i^t) = (p_{j_1} \cdots p_{j_M}, q_i)$ für $i = 1, \ldots, l$ und $t \geq 2$. □

Man betrachte nun den Fall, in dem $m_i = p_j^{\alpha_j}$ für $1 \leq i \leq l$ und $j \in \{1, \ldots, l\}$ gilt.

Satz 5.6 *Seien $p_1, \ldots, p_l$ verschiedene Primzahlen und $\varepsilon_1, \ldots, \varepsilon_l \in \left\{0, 1, \ldots, p_j^{\alpha_j} - 1\right\}$ für ein $j \in \{1, \ldots, l\}$ und eine positive ganze Zahl α_j. Dann gilt*

$$\left|\left\{0 \leq n < N : e_{p_i}(n!) \equiv \varepsilon_i \bmod p_j^{\alpha_j},\ 1 \leq i \leq l\right\}\right| = \frac{N}{p_j^{\alpha_j l}} + \mathcal{O}\left(N^{1-\delta}\right)$$

mit $\delta = \frac{1}{120 l^2 \overline{p}^{3p_j^{\alpha_j}} p_j^{2\alpha_j}}$, wobei $\overline{p} = \max_{1 \leq i \leq l} p_i$ sei.

Beweis. Definiere für $i = 1, \ldots, l$ mit $i \neq j$ die Funktionen f_i wie im Beweis von Satz 5.1. Dann gilt wiederum $f_i(n) \equiv e_{p_j}(n!)$ für $i = 1, \ldots, l$ mit $i \neq j$. Definiere

$f_j(n) = S_{p_j}(n)$. Mit (5.7) gilt

$$\begin{aligned} e_{p_j}(n!) &= \sum_{k=1}^{s} \left(n_k p_j^{k-1} + n_k p_j^{k-2} + \cdots + n_k p_j + n_k\right) \\ &\equiv \sum_{k=1}^{s} \left(n_k p_i^{\alpha_j - 1} + \cdots + n_k p_j + n_k\right) \mod p_j^{\alpha_j} \\ &\equiv p_i^{\alpha_j-1}(S_{p_j}(n) - n_0) + \cdots + p_j(S_{p_j}(n) - n_0) + (S_{p_j}(n) - n_0) \mod p_j^{\alpha_j} \\ &\equiv \left(p_i^{\alpha_j-1} + \cdots + p_j + 1\right)(S_{p_j}(n) - n_0) \mod p_j^{\alpha_j}. \end{aligned}$$

Da nun

$$\left(p_i^{\alpha_j-1} + \cdots + p_j + 1\right)(1 - p_j) = 1 - p_i^{\alpha_j} \equiv 1 \mod p_i^{\alpha_j}$$

gilt, kann man mit der genannten Definition von $\mathbf{f}$ also das Kongruenzsystem

$$f_i(n) \equiv \begin{cases} \varepsilon_i \mod p_j^{\alpha_j} & \text{für } i = 1, \ldots, l \text{ mit } i \neq j \\ \varepsilon_i(1 - p_j) + n_0 \mod p_j^{\alpha_j} & \text{sonst,} \end{cases}$$

betrachten. Sei $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{j-1}, \varepsilon_j(1 - p_j) + n_0, \varepsilon_{j+1}, \ldots, \varepsilon_l)$, wobei die j-te Komponente mod $p_j^{\alpha_j}$ betrachtet wird. Dann gilt mit Korollar 4.12 und Lemma 5.2

$$\begin{aligned} &\left|\left\{0 \le n < N : \ e_{p_i}(n!) \equiv \varepsilon_i \bmod p_j^{\alpha_j} \ (1 \le i \le l)\right\}\right| \\ &\quad = \left|\left\{0 \le n < N : \mathbf{f}(n) \equiv \varepsilon \bmod p_j^{\alpha_j}\right\}\right| \\ &\quad = \left|\left\{0 \le \nu < \left[\frac{N}{p_j}\right] + \kappa_0 : \mathbf{f}(p_j\nu) \equiv \varepsilon \bmod p_j^{\alpha_j}\right\}\right| \\ &\qquad + \left|\left\{0 \le \nu < \left[\frac{N}{p_j}\right] + \kappa_1 : \mathbf{f}(p_j\nu + 1) \equiv \varepsilon \bmod p_j^{\alpha_j}\right\}\right| \\ &\qquad + \cdots + \left|\left\{0 \le \nu < \left[\frac{N}{p_j}\right] + \kappa_{p_j-1} : \mathbf{f}(p_j\nu + p_j - 1) \equiv \varepsilon \bmod p_j^{\alpha_j}\right\}\right| \\ &\quad = \frac{\left[\frac{N}{p_j}\right] + \kappa_0}{p_j^{\alpha_j l}} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_0\right)^{1-\delta}\right) \\ &\qquad + \frac{\left[\frac{N}{p_j}\right] + \kappa_1}{p_j^{\alpha_j l}} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_1\right)^{1-\delta}\right) \\ &\qquad + \cdots + \frac{\left[\frac{N}{p_j}\right] + \kappa_{p_j-1}}{p_j^{\alpha_j l}} + \mathcal{O}\left(\left(\left[\frac{N}{p_j}\right] + \kappa_{p_j-1}\right)^{1-\delta}\right) \\ &\quad = \frac{N}{p_j^{\alpha_j l}} + \mathcal{O}\left(N^{1-\delta}\right). \end{aligned}$$

Mit $q_i = p_i^{\lambda_i}$ für $i = 1, \ldots, l$ und $i \neq j$ und $q_j = p_j$ ist f_i für alle i vollständig q_i-additiv. Es gilt $\mathbf{u} = (p_j, \ldots, p_j)$, woraus sich ergibt, dass $\left(u_j, q_j^{t_j}\right) = \left(p_j, p_j^{t_j}\right) = (p_j, p_j) = (u_j, q_j)$ ist sowie $\left(u_i, q_i^{t_i}\right) = \left(p_j, p_i^{\lambda_i t_i}\right) = \left(p_j, p_i^{\lambda_i}\right) = (u_i, q_i)$ für alle $i \neq j$ gilt, da p_i und p_j teilerfremd sind. Außerdem gilt $F_j = f_j(1) = 1$ und $F_i = f_i(1) = 0$ für $i = 1, \ldots, l$ und $i \neq j$ und $d_j = \left(p_j^{\alpha_j}, p_j - 1\right) = 1$. Wähle $r = p_i$ für $i \neq j$. Dann gilt erneut $f_i(r) - rF_i = 1$ für $i \neq j$. Damit ist also auch für $i \neq j$ $d_i = 1$ und die Voraussetzungen von Korollar 4.12 sind erfüllt. Damit folgt der Satz. □

Bemerkung 5.7 Ähnlich wie in Satz 5.5 kann nun noch der Fall betrachtet werden, in dem ein Teil der Moduli m_i gleich einer Primzahlpotenz ist und für die restlichen $p_i \nmid m_i$ gilt. Hier muss der Beweis nur in sofern abgeändert werden, dass das Kongruenzsystem

$$f_i(n) \equiv \begin{cases} a_i \mod m_i & \text{für } i \neq j_\mu \\ a_i(1 - p_i) + n_0 \mod p_i^{\alpha_i} & \text{sonst,} \end{cases}$$

betrachtet wird, wobei f_i im Fall $i = j_\mu$ durch S_{p_i} definiert sei und andernfalls durch die von Luca und Stănică definierte Funktion aus Satz 5.1. Setzt man

$$a_i^* = \begin{cases} a_i & \text{falls } i \neq j_\mu \\ a_i(1 - p_i) + n_0 & \text{falls } i = j_\mu \end{cases}$$

und $p = p_{j_1} \cdots p_{j_M}$, so erhält man die entsprechende Abschätzung, da auch hier die Voraussetzungen von Korollar 4.12 erfüllt sind.

Bemerkung 5.8 Wie bereits erwähnt, eignet sich die Ziffernsumme im allgemeinen Fall nicht, da sich die Kongruenz zu $e_{p_i}(n!)$ modulo m_i im Allgemeinen nicht passend formulieren lässt. Hierfür betrachte man zum Beispiel

$$\begin{aligned} e_2(n!) &= \sum_{k=0}^{s} n_k \left(2^k - 1\right) \\ &= n_1 + 3n_2 + 7n_3 + 15n_4 + 31n_5 + \cdots \\ &\equiv n_1 + 3n_2 + n_3 + 3n_4 + n_5 + \cdots \mod 6 \\ &\equiv S_2(n) - n_0 + 2 \sum_{\substack{k=2 \\ 2 \mid k}}^{s} n_k \mod 6. \end{aligned}$$

Eine Fallunterscheidung, wie sie in den voran gegangene Beweisen vorgenommen wurde, ist hier nicht möglich. Auch kann $S_2(n) + 2 \sum_{\substack{k=2 \\ 2 \mid k}}^{s} n_k$ nicht als Funktion verwendet werden, da diese laut Bemerkung 2.2 nicht vollständig 2-additiv ist.

5.3 Der allgemeine Fall $\mathbf{m_i = k_i p_i^{\alpha_i}}$

Nun wird der allgemeine Fall $m_i = k_i p_i^{\alpha_i}$ mit $(k_i, p_i^{\alpha_i}) = 1$ betrachtet. Dieser wurde von Berend und Kolesnik [2] bearbeitet. Da aus dem Beweis nicht klar hervor geht, wie die Aussage für $\alpha_i = 1$ folgt, wird dies hier ausgeschlossen.

Satz 5.9 [2, Theorem 2.1] *Seien* $\mathbf{a} = (a_1, \ldots, a_l)$ *und* $\mathbf{m} = (m_1, \ldots, m_l)$ *l-Tupel mit ganzzahligen Einträgen. Man schreibe* $m_j = k_j p^{\alpha_j}$ *mit* $\left(k_j, p_j^{\alpha_j}\right) = 1$. *Es sei* $\alpha_j > 1$ *für alle* j, *dann gilt*

$$\left|\left\{0 \le n < N : e_{p_j}(n!) \equiv a_j \bmod m_j \ (j = 1, \ldots, l)\right\}\right| = \frac{N}{m_1 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right), \tag{5.9}$$

wobei $\delta = \frac{4}{\overline{q}^2 \overline{m}^2 l \log \overline{q} + 8l + 8}$ *ist, mit* $\overline{q} = \max_{\le i \le l} q_i$ *und* $\overline{m} = \max_{\le i \le l} m_i$.

Beweis. Seien $p_1, \ldots, p_l$ unterschiedliche Primzahlen und $m_1, \ldots, m_l$ positive ganze Zahlen größer 2. In [2] werden die folgenden vier Fälle unterschieden:

1. Fall: $\alpha_j = 1$ und $k_j = 1$. Hierbei handelt es sich um den Fall, dass der Modul eine Primzahl ist. Definiere $u_j = 2$ und $\beta_j = 2$.

2. Fall: $\alpha_j \ge 2$ und $k_j = 1$. In diesem Fall ist m_j eine Primzahlpotenz. Definiere $u_j = 1$ und $\beta_j = \alpha_j$.

3. Fall: $\alpha_j = 0$ und $k_j > 1$. Hier gilt $m_j \nmid p_j$. Dieser Fall wurde bereits von Luca und Stănică [16] betrachtet und bewiesen. Hier sei u_j die kleinste positive ganze Zahl mit

$$\frac{p_j^{u_j} - 1}{p_j - 1} \equiv 0 \mod k_j$$

und $\beta_j = u_j$.

4. Fall: $\alpha_j \ge 1$ und $k_j > 1$. u_j sei wie im 3. Fall definiert und es sei $\beta_j = KgV(\alpha_j, u_j)$.

Im folgenden sein nun jedoch $\alpha_j > 1$.

Man definiere nun für $1 \le j \le l$ die vollständig q_j-additiven Funktionen f_j, wobei $q_j = p_j^{u_j}$ sei, durch

$$f_j(n) = 0, \qquad n = 0, 1, \ldots,$$

falls $k_j = 1$ ist und durch

$$f_j(n) = e_{p_j}(n!), \qquad n = 0, 1, \ldots, q_j - 1$$

andernfalls. Wie bereits in Kapitel 2 erwähnt, ist eine vollständig q-additive Funktion f durch die Angabe der Werte $f(0), f(1), \ldots, f(q-1)$ eindeutig festgelegt. Damit genügt es auch hier, die ersten q_j Werte für f_j anzugeben. Setze nun

$$v_j = \frac{p_j^{\alpha_j} - 1}{p_j - 1}, \qquad 1 \leq j \leq l$$

und definiere g_j durch

$$g_j(n) = e_{p_j}(n!) + v_j n, \qquad n = 0, 1, \ldots.$$

Nun definiere für $1 \leq j \leq l$ die vollständig q_{l+j}-additiven Funktionen f_j, wobei $q_{l+j} = p^{\alpha_j}$ sei, durch

$$f_{l+j}(n) = g_j(n), \qquad n = 0, 1, \ldots, q_{l+j} - 1,$$

falls $\alpha_j \geq 2$ und durch

$$f_{l+j}(n) = 0, \qquad n = 0, 1, \ldots,$$

falls $\alpha_j = 0$. Im Folgenden werden die Fälle betrachtet, in denen f_j und f_{l+j} nicht der Nullfunktion entsprechen. Nun ist zu zeigen, dass die Kongruenz

$$f_{l+j}(n) \equiv g_j(n) \mod q_{l+j}, \qquad 1 \leq j \leq l, n = 0, 1, \ldots \tag{5.10}$$

gilt. Aufgrund der Definition von f_{l+j} ist dies für Zahlen $0, \ldots, q_{l+j}$ offensichtlich. Man nehme nun an, dass die Kongruenz für alle $n_0 < n$ gilt und schreibe n in der Form $n = cq_{l+j} + d$ für ganze Zahlen $c \geq 1$ und $0 \leq d \leq q_{l+q} - 1$. Die p_j-adischen Entwicklungen von c und d seien gegeben durch

$$c = \sum_{i=0}^{t} c_i p_j^i, \qquad d = \sum_{i=0}^{\alpha_j - 1} d_i p_j^i.$$

Da f_{l+j} vollständig q_{l+j}-additiv ist und mit (5.6) gilt dann

$$\begin{aligned}
f_{l+j}(n) &= f_{l+j}(c) + f_{l+j}(d) \\
&\equiv e_{p_j}(c!) + v_j c + e_{p_j}(d!) + v_j d \mod q_{l+j} \\
&= \sum_{i=0}^{t} c_i \frac{p_j^i - 1}{p_j - 1} + v_j c + e_{p_j}(d!) + v_j d \\
&\equiv \sum_{i=0}^{t} c_i \frac{p_j^i - 1}{p_j - 1} + v_j c + v_j c q_{l+j} + e_{p_j}(d!) + v_j d \mod q_{l+j} \\
&= \sum_{i=0}^{t} c_i \frac{p_j^i - 1}{p_j - 1} + \sum_{i=0}^{t} c_i \frac{p_j^{\alpha_j+i} - p_j^i}{p_j - 1} + v_j(cq_{l+j} + d) + e_{p_j}(d!) \\
&= \sum_{i=0}^{t} c_i \frac{p_j^{\alpha_j+i} - 1}{p_j - 1} + \sum_{i=0}^{\alpha_j-1} d_i \frac{p_j^i - 1}{p_j - 1} + v_j(cq_{l+j} + d) \\
&= \sum_{i=\alpha_j}^{t+\alpha_j} c_{i-\alpha_j} \frac{p_j^i - 1}{p_j - 1} + \sum_{i=0}^{\alpha_j-1} d_i \frac{p_j^i - 1}{p_j - 1} + v_j(cq_{l+j} + d) \\
&= e_{p_j}((cq_{l+j} + d)!) + v_j(cq_{l+j} + d),
\end{aligned}$$

womit die Behauptung bewiesen ist.

Setze nun $q = \prod_{j=1}^{l} q_{l+j}$. Für $a = 1, \ldots, q-1$ sei

$$R(a) = \left\{0 \le n < N : n \equiv a \bmod q,\ e_{p_j}(n!) \equiv a_j \mod m_j (1 \le j \le l)\right\}.$$

Bezeichne $N(\mathbf{a})$ die linke Seite von (5.9). Es gilt $N(\mathbf{a}) = \sum_{a=0}^{q-1} |R(a)|$, so dass es also genügt

$$|R(a)| = \frac{N}{qm_1 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right)$$

zu zeigen. Setzt man nun $b_j = a \mod q_{j+l}$ für $1 \le j \le l$, dann gilt

$$\begin{aligned}
R(a) = \big\{0 \le n < N : n \equiv a \bmod q,\ & f_j(n) \equiv a_j \bmod k_j, \\
& f_{l+j}(n) \equiv a_j + v_j b_j \bmod q_{l+j}\ (1 \le j \le l)\big\},
\end{aligned} \tag{5.11}$$

da $\left(k_j, p_j^{\alpha_j}\right) = 1$ ist.

Da β_j von u_j und α_j geteilt wird, sind die Funktionen f_j und f_{l+j} beide vollständig $p_j^{\beta_j}$-additiv. Außerdem gilt $\beta_j \ge 2$ und somit $p_j^{\beta_j} \ge 3$ Nun ist noch zu zeigen, dass die weiteren Voraussetzungen von Satz 4.15, also die Gleichungen (4.40) und (4.41) erfüllt

sind. Es gilt $f_j(p_j) = e_{p_j}(p_j!) = 1$ und $f_j(1) = 0$, womit (4.40) gezeigt ist. Außerdem gilt

$$\begin{aligned} f_{l+j}(p_j) - p_j f_{l+j}(1) &= e_{p_j}(p_j!) + v_j p_j - p_j \left(e_{p_j}(1) + v_j\right) \\ &= 1 + v_j p_j - p_j v_j = 1, \end{aligned}$$

womit auch (4.41) gezeigt ist.

Nun gilt laut Satz 4.15

$$\begin{aligned} |R(a)| &= \frac{N}{qk_1 p_1^{\alpha_1} \cdots k_l p_l^{\alpha_l}} + \mathcal{O}\left(N^{1-\delta}\right) \\ &= \frac{N}{qm_1 \cdots m_l} + \mathcal{O}\left(N^{1-\delta}\right), \end{aligned} \tag{5.12}$$

falls alle $\alpha_j > 1$ sind. □

Bemerkung 5.10 Berend und Kolesnik setzen in ihrem Beweis $q_{l+j} = p^2$, falls $\alpha_j = 1$ ist. In diesem Fall gilt $k_j q_{l+j} = k_j p_j^2 \neq k_j p_j$, womit im Nenner des Bruchs in (5.12) zusätzliche Faktoren p_i auftreten. Diese Definition von p_{l+j} für den Fall $\alpha_j = 1$ bleibt unklar, zumal die vollständige q_j-Additivität, die für die Verwendung des Satzes 4.15 benötigt wird, bereits durch die Wahl von $q_j = p_j^{\beta_j}$ gegeben ist.

5.4 Über den Fehlerterm

Abschließend kann nun noch die Frage gestellt werden, ob der Fehlerterm $\mathcal{O}\left(N^{1-\delta}\right)$ noch deutlich verbessert werden kann. Es werden drei Beispiele betrachtet. Das erste Beispiel, welches [2] entnommen ist, verdeutlicht, dass der Fehler auch sehr klein sein kann. Im zweiten Beispiel ist der Fehler $\Omega_{\pm}(\sqrt{N})$, weshalb der Fehlerterm im Allgemeinen nicht deutlich verbessert werden kann. Das dritte Beispiel gibt eine Abschätzung für $|\{0 \leq n < N : n \equiv 0 \bmod 6, e_2(n!) \equiv 0 \bmod 2\}|$ an, die bezüglich des Fehlerterms etwas besser ist, als die, die man mit Korollar 4.12 erhalten kann.

Beispiel 5.11 Betrachte die Folge $(e_2(n!) \bmod 2)_{n=0}^{\infty}$. Im Fall $4|n$ gilt $e_2((n+1)!) = e_2(n!)$ und $e_2((n+2)!) = e_2((n+3)!) = e_2(n!) + 1$. Hieraus folgt, dass 4 aufeinander

folgende Folgenglieder, wobei das erste Folgenglied so gewählt sei, dass $4|n$, zwei Nullen und zwei Einsen sind. Also ist der Fehlerterm hier durch 1 beschränkt. Für die Folge $(e_p(n!) \bmod 2)_{n=0}^{\infty}$, wobei p eine Primzahl bezeichne, ist die Situation entsprechend.

Das folgende Beispiel wurde in [2] für den Fall $p = 3$ angeführt und wird hier für den allgemeinen Fall, wobei $p \neq 2$ wiederum eine Primzahl bezeichne, vorgestellt.

Beispiel 5.12 Betrachte die Folge $(e_p(n!) \bmod 2)_{n=0}^{\infty}$ mit $p \neq 2$. Man erhält mit $r = 0, 1, \ldots, p^2 - 1$

$$\begin{aligned} e_p\left((p^2n + r!)\right) &= \left[\frac{p^2n + r}{p}\right] + \left[\frac{p^2n + r}{p^2}\right] + \left[\frac{p^2n + r}{p^3}\right] + \ldots \\ &= pn + \left[\frac{r}{p}\right] + n + e_p(n!) \\ &= (p+1)n + \left[\frac{r}{p}\right] + e_p(n!) \\ &\equiv \left[\frac{r}{p}\right] + e_p(n!) \mod 2. \end{aligned} \tag{5.13}$$

Im Bereich $[0, p^2 - 1]$ sind $\frac{p(p+1)}{2}$ der Werte, die von $\left[\frac{r}{p}\right]$ angenommen werden, gleich 0 und $\frac{p(p-1)}{2}$ der Werte sind gleich 1. Sei nun a_s die Anzahl der Nullen und b_s die Anzahl der Einsen in der endlichen Folge $(e_p(n!) \bmod 2)_{n=0}^{p^{2s}-1}$. Dann folgt aus (5.13)

$$a_{s+1} = \frac{p(p+1)}{2}a_s + \frac{p(p-1)}{2}b_s, \qquad b_{s+1} = \frac{p(p-1)}{2}a_s + \frac{p(p+1)}{2}b_s.$$

Hieraus folgt mit vollständiger Induktion, dass

$$a_s = \frac{p^{2s} + p^s}{2}, \qquad b_s = \frac{p^{2s} - p^s}{2}. \tag{5.14}$$

Für $s = 1$ gilt (5.14) offensichtlich. Man nehme nun an, dass (5.14) gilt. Dann ergibt sich

$$\begin{aligned} a_{s+1} &= \frac{p(p+1)}{2}a_s + \frac{p(p-1)}{2}b_s \\ &= \frac{p(p+1)}{2} \cdot \frac{p^{2s} + p^s}{2} + \frac{p(p-1)}{2} \cdot \frac{p^{2s} - p^s}{2} \\ &= \frac{(p^2+p)(p^{2s} + p^s)}{4} + \frac{(p^2-p)(p^{2s} - p^s)}{4} \\ &= \frac{2p^{2s+2} + 2p^{s+1}}{4} = \frac{p^{2(s+1)} + p^{s+1}}{2} \end{aligned}$$

und

$$\begin{aligned} b_{s+1} &= \frac{p(p-1)}{2}a_s + \frac{p(p+1)}{2}b_s \\ &= \frac{p(p-1)}{2}\cdot\frac{p^{2s}+p^s}{2} + \frac{p(p+1)}{2}\cdot\frac{p^{2s}-p^s}{2} \\ &= \frac{(p^2-p)(p^{2s}+p^s)}{4} + \frac{(p^2+p)(p^{2s}-p^s)}{4} \\ &= \frac{2p^{2s+2}-2p^{s+1}}{4} = \frac{p^{2(s+1)}-p^{s+1}}{2}. \end{aligned}$$

Damit gilt

$$\frac{p^{2s}+p^s}{2} - \frac{p^2 s-1}{2} = \frac{p^s}{2} = \sqrt{p^{2s}}$$

und

$$\frac{p^{2s}-p^s}{2} - \frac{p^2 s-1}{2} = -\frac{p^s}{2} = -\sqrt{p^{2s}}$$

woraus folgt, dass der Fehlerterm hier $\Omega_{\pm}(\sqrt{N})$ ist.

Das letzte Beispiel ist wiederum [2] entnommen und wird hier etwas ausführlicher vorgestellt.

Beispiel 5.13 Man betrachte nun die Ziffern der dyadischen Entwicklung eines Vielfachen von 3. $D(n)$ sei die Anzahl der Einsen der dyadischen Entwicklung von n und $S(N)$ sei durch

$$S(N) = \sum_{0\le j\le \frac{N}{3}} (-1)^{D(N-3j)}, \qquad \alpha = \frac{\log 3}{\log 4}$$

definiert. Newman [17] bewies, dass dann

$$\frac{1}{20}n^{\alpha} < S(3n) < 5n^{\alpha}$$

gilt. Da für positive ganze Zahlen n mit $n \equiv 0 \bmod 2$ laut (5.8) $e_2(n!) \equiv S_2(n)$ gilt, folgt hieraus direkt, dass

$$|\{0 \le n < N : n \equiv 0 \bmod 6, e_2(n!) \equiv 0 \bmod 2\}| = \frac{N}{6} + \mathcal{O}\left(N^{\log_4 3}\right)$$

gilt.

Laut Korollar 4.12 und mit Lemma 5.2 gilt

$$\begin{aligned}
&|\{0 \le n < N :\ n \equiv 0 \bmod 6, e_2(n!) \equiv 0 \bmod 2\}| \\
&\qquad = |\{0 \le n < N : n \equiv 0 \bmod 6, S_2(n) \equiv 0 \bmod 2\}| \\
&\qquad = \left|\left\{0 \le \nu < \left[\frac{N}{6} + \kappa_0\right] : S_2(6\nu) \equiv 0 \bmod 2\right\}\right| \\
&\qquad = \frac{N}{6} + \mathcal{O}\left(N^{1-\delta}\right),
\end{aligned}$$

mit $\delta = \frac{1}{120 \cdot 2^5}$.

Index

Literaturverzeichnis

[1] Berend, D.: On the parity of exponents in the factorization of $n!$. In: *J. Number Theory* 64 (1997), Nr. 1, S. 13–19. – ISSN 0022–314X

[2] Berend, D. ; Kolesnik, G.: *Regularity of patterns in the factorization of n!* 2006. – J. Number Theory, doi:10.1016/j.jnt2006.08.010

[3] Bésineau, J.: Indépendance statistique d'ensembles liés à la fonction "somme des chiffres". In: *Acta Arith.* 20 (1972), S. 401–416. – ISSN 0065–1036

[4] Chen, Y.-G.: On the parity of exponents in the standard factorization of $n!$. In: *J. Number Theory* 100 (2003), Nr. 2, S. 326–331. – ISSN 0022–314X

[5] Chen, Y.-G. ; Zhu, Y.-C.: On the prime power factorization of $n!$ In: *J. Number Theory* 82 (2000), Nr. 1, S. 1–11. – ISSN 0022–314X

[6] Coquet, J.: Power sums of digital sums. In: *J. Number Theory* 22 (1986), Nr. 2, S. 161–176. – ISSN 0022–314X

[7] Delange, H.: Sur les fonctions q-additives ou q -multiplicatives. In: *Acta Arith.* 21 (1972), S. 285–298. (errata insert). – ISSN 0065–1036

[8] Erdős, P. ; Graham, R. L.: *Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique]*. Bd. 28: *Old and new problems and results in combinatorial number theory*. Geneva : Université de Genève L'Enseignement Mathématique, 1980. – 128 S.

[9] Erdös, P. ; Kac, M.: The Gaussian law of errors in the theory of additive number theoretic functions. In: *Amer. J. Math.* 62 (1940), S. 738–742. – ISSN 0002–9327

[10] Gelfond, A. O.: Sur les nombres qui ont des propriétés additives et multiplicatives données. In: *Acta Arith.* 13 (1967/1968), S. 259–265. – ISSN 0065–1036

[11] Grabner, P. J.: Completely q-multiplicative functions: the Mellin transform approach. In: *Acta Arith.* 65 (1993), Nr. 1, S. 85–96. – ISSN 0065–1036

[12] Graham, S.W. ; Kolesnik, G.: *Van der Corput's method for exponential sums.* London Mathematical Society Lecture Note Series, 126. Cambridge etc.: Cambridge University Press. 120 p., 1991

[13] Kátai, I.: Distribution of q-additive function. In: *Probability theory and applications* Bd. 80. Dordrecht : Kluwer Acad. Publ., 1992, S. 309–318

[14] Kim, Dong-Hyun: On the joint distribution of q-additive functions in residue classes. In: *J. Number Theory* 74 (1999), Nr. 2, S. 307–336. – ISSN 0022–314X

[15] Kuipers, L. ; Niederreiter, H.: *Uniform distribution of sequences.* New York : Wiley-Interscience [John Wiley & Sons], 1974. – xiv+390 S. – Pure and Applied Mathematics

[16] Luca, F. ; Stănică, P.: On the prime power factorization of $n!$ In: *J. Number Theory* 102 (2003), Nr. 2, S. 298–305. – ISSN 0022–314X

[17] Newman, D. J.: On the number of binary digits in a multiple of three. In: *Proc. Amer. Math. Soc.* 21 (1969), S. 719–721. – ISSN 0002–9939

[18] Sander, J. W.: On the parity of exponents in the prime factorization of factorials. In: *J. Number Theory* 90 (2001), Nr. 2, S. 316–328. – ISSN 0022–314X

[19] Shapiro, H. N.: *Introduction to the theory of numbers.* New York : John Wiley & Sons Inc., 1983 (Pure and Applied Mathematics). – xii+459 S. – ISBN 0–471–86737–3. – , A Wiley-Interscience Publication

[20] Thuswaldner, J. M. ; Tichy, R. F.: An Erdős-Kac theorem for systems of q-additive functions. In: *Indag. Math. (N.S.)* 11 (2000), Nr. 2, S. 283–291. – ISSN 0019–3577

[21] Weyl, H.: Über die Gleichverteilung von Zahlen mod. Eins. In: *Math. Ann.* 77 (1916), Nr. 3, S. 313–352. – ISSN 0025–5831

Lebenslauf

Name	Iris Lieske
Geburtsdatum/-ort	23. Februar 1978, Höxter

Schulbildung

08/1984–06/1988	Grundschule Beverungen
08/1988–06/1997	Städtisches Gymnasium Beverungen
03.06.1997	Abitur

Studium

10/1997–07/2003	Lehramt an Gymnasien, Universität Hannover, Fächer: Mathematik, Biologie
21.07.2003	1. Staatsexamen
04/2001–10/2003	Mathematik mit Nebenfach Biologie, Universität Hannover
28.10.2003	Diplom-Mathematikerin, Diplomarbeit zum Thema „Cantormengen und Kettenbrüche“

Berufstätigkeit

1999–2003	Studentische Hilfskraft am Institut für Mathematik der Universität Hannover
05/2001–08/2001	Studentische Hilfskraft der Firma FirstMark Communication GmbH
11/2003–05/2004	Studienreferendarin am Gymnasium am Silberkamp, Peine
06/2004–heute	Wissenschaftliche Mitarbeiterin bei der Einrichtung uniKIK der Leibniz Universität Hannover