Georg-August-Universität Göttingen
Fakultät für Mathematik und Informatik
Mathematisches Institut
Wintersemester 2020/21

Lösungen der Gleichungen $\phi(n) = \phi(n+h)$ und $\sigma(n) = \sigma(n+h)$ sowie deren Übertrag auf algebraische Ganzheitsringe

Johann Christian Stumpenhusen
Matrikelnummer: 21675783
E-Mail: j.stumpenhusen@stud.uni-goettingen.de
B. Sc. Mathematik
8. Fachsemester
Betreuerin: Univ.-Prof. Dr. Damaris Schindler
Zweitgutachter: Univ.-Prof. Dr. Preda Mihăilescu
Abgabetermin: 30. März 2021

Inhaltsverzeichnis

1 Einleitung

In der Zahlentheorie beschäftigen wir uns unter anderem mit der Relation $a \mid b$, wobei a und b Elemente der natürlichen Zahlen $\mathbb{N}$ sind. Es gibt es zwei sehr bekannte Funktionen auf den natürlichen Zahlen, die sich dieser Relation bedienen und Verwendung in vielen Resultaten der Zahlentheorie finden.

Definition 1.0.1. Seien $a, b, d \in \mathbb{N}$. Wir definieren einige Grundbegriffe:

1. Der *größte gemeinsame Teiler* $(a, b) = d$ von a und b ist diejenige natürliche Zahl, sodass $d|a$ und $d|b$ und gleichzeitig für $c \in \mathbb{N}$ aus $c|a$ und $c|b$ stets $c|d$ folgt.
2. Die (Euler'sche) ϕ-Funktion $\phi(a) = |\{x \leq a : (x, a) = 1\}|$ zählt die zu a teilerfremden natürlichen Zahlen kleiner als a.
3. Die Teilersummenfunktion $\sigma(a) = \sum_{x\in\mathbb{N},\, x|a} x$ summiert alle natürlichen Teiler von a auf.

Wir wollen uns mit der nachstehenden Hypothese für $h \in \mathbb{N}$ beschäftigen, zu der Kevin Ford [5] ein qualitatives Ergebnis erzielte.

Hypothese $\mathcal{S}_h$. Es gibt unendlich viele $n \in \mathbb{N}$, sodass $\phi(n) = \phi(n + h)$.

Diese Hypothese würde für sämtliche $h \in \mathbb{N}$ aus einer älteren Vermutung von Erdős über konsekutive Zahlen mit gleichen Totienten folgen.

Vermutung 1.0.2. (Erdős) Sei $h \in \mathbb{N}$. Dann gilt

$$\phi(n) = \phi(n + 1) = \ldots = \phi(n + h - 1)$$

für unendlich viele $n \in \mathbb{N}$.

Ford führt zu Beginn seiner Arbeit aus, dass zuvor nur numerische Schätzungen und ein paar Vermutungen zu $\mathcal{S}_h$ existierten, aber keine konkreten Lösungen. Er benutzt hierfür ein Ergebnis von Maynard [10] und vom PolyMath8b Projekt [12], um ein h zu konstruieren, für das $\mathcal{S}_h$ gilt.

Da wir über den natürlichen Zahlen $\mathbb{N}$ die Äquivalenzen

$$p \text{ ist prim} \iff \phi(p) = p - 1 \iff \sigma(p) = p + 1$$

haben, lassen sich häufig Resultate über die Euler'sche ϕ-Funktion auf Aussagen der Teilersummenfunktion σ übertragen. Dies ist in diesem Fall wegen der andersartigen expliziten Form der beiden Funktionen nicht möglich, jedoch beschäftigt sich Ford in [5] auch mit der folgenden ähnlichen Hypothese.

Hypothese $\mathcal{T}_h$. Es gibt unendlich viele $n \in \mathbb{N}$, sodass $\sigma(n) = \sigma(n+h)$.

In der algebraischen Zahlentheorie beschäftigen wir uns mit den Ringen in einer Zahlkörpererweiterung $K/\mathbb{Q}$, die sich zu K verhalten wie $\mathbb{Z}$ zu $\mathbb{Q}$.

Definition 1.0.3. Sei $R \subset S$ ein Ringturm. Ein Element $s \in S$ heißt *ganz* über R, falls es eine Nullstelle eines monischen Polynoms $f \in R[x]$ ist. Für einen algebraischen Zahlkörper K (das heißt: $[K : \mathbb{Q}] < \infty$) bezeichnen wir die Elemente in K, die ganz über $\mathbb{Z}$ sind, als Ganzheitsring $\mathcal{O}_K$ von K. Diese bilden selber einen Ring.

Die Eulerfunktion ϕ kann für ein $\alpha \in \mathcal{O}_K$ für eine algebraische Zahlkörpererweiterung $K/\mathbb{Q}$ über die Definition

$$\phi_K(\alpha) = \left|\left({}^{\mathcal{O}_K}/_{\langle\alpha\rangle}\right)^*\right|,$$

wobei $\langle\alpha\rangle$ das von α in $\mathcal{O}_K$ erzeugte Ideal ist, sowie die Teilersummenfunktion σ über

$$\sigma_K(\alpha) = \sum_{\mathfrak{b} \supset \langle\alpha\rangle} \left|{}^{\mathcal{O}_K}/_{\mathfrak{b}}\right|$$

auf jeden algebraischen Zahlkörper K übertragen werden [8, S. 30]. Wir wollen überprüfen, welche Elemente die äquivalenten Hypothesen in einer algebraischen Zahlkörpererweiterung $K/\mathbb{Q}$ erfüllen. Es sei $h \in \mathcal{O}_K$ und wir definieren:

Hypothese $\mathcal{S}_{h,K}$. Es gibt unendlich viele $\alpha \in \mathcal{O}_K$, sodass $\phi_K(\alpha) = \phi_K(\alpha + h)$.

Hypothese $\mathcal{T}_{h,K}$. Es gibt unendlich viele $\alpha \in \mathcal{O}_K$, sodass $\sigma_K(\alpha) = \sigma_K(\alpha + h)$.

Wir werden zeigen, dass unter Annahme einer Vermutung von Schinzel $S_{h,K}$ für alle komplexen quadratischen Körpererweiterungen von $\mathbb{Q}$ und $h \in \mathcal{O}_K$ mit

$$2^{13}3^7 5^4 7^4 11^3 13^3 17^3 19^3 23^3 \prod_{p \in \mathbb{P},\, 29 \le p \le 47} p \mid h$$

gilt, wobei wir mit $\mathbb{P}$ die Menge der Primzahlen in $\mathbb{N}$ bezeichnen.

Zuletzt wollen wir uns kurz damit beschäftigen, was wir darüber sagen können, wenn wir n und $n+h$ in den Hypothesen $\mathcal{S}_h$ und $\mathcal{T}_h$ durch allgemeinere lineare Formen $a_1 n + b_1$

und $a_2n + b_2$ aus $\mathbb{Z}[x]$ ersetzen. Dabei werden wir zeigen, dass es ein $h \leq 227950$ gibt, sodass für alle ungeraden $l \in \mathbb{N}$ die Gleichung

$$\phi(n) = \phi(2n + 2lh)$$

unendlich viele Lösungen $n \in \mathbb{N}$ besitzt.

1.1 Bisherige Arbeiten und Ergebnisse

Neben Ford [5] beschäftigten sich auch Graham, Holt und Pomerance [13] mit der Hypothese $\mathcal{S}_h$. Ersterer bezieht sich in seiner Arbeit auch ausdrücklich auf den von letzteren Autoren genannten Fall, dass, sofern j und $j + h$ dieselben Primfaktoren haben und

$$\frac{j}{(j, j+h)}r + 1 \quad \text{und} \quad \frac{j+h}{(j, j+h)}r + 1$$

für ein $r \in \mathbb{N}$ prim sind, für

$$n = j(\frac{j+h}{(j, j+h)}r + 1)$$

die Gleichung $\phi(n) = \phi(n + h)$ erfüllt ist. Die in [5] vorgestellte Lösung für $\mathcal{S}_h$ erinnert in ihrer Konstruktion hieran.

Verschiedene Autoren haben sich zudem damit beschäftigt, für je ein festes $h \in \mathbb{N}$ und eine Schranke $N \in \mathbb{N}$ diejenigen $n \leq N$ zu berechnen, für die $\phi(n) = \phi(n + h)$ gilt, insbesondere für $h = 1$ oder $h \equiv 0 \mod 2$.[1] Für die Vermutung 1.0.2 von Erdős sieht die numerische Lage sehr spärlich aus: Falls $m \geq 3$, so ist nur der Fall $n = 5186$ und $m = 3$ bekannt. Wie Graham, Holt und Pomerance feststellten, sind Lösung von $\phi(n) = \phi(n+h)$ für $n \leq 10^{10}$ besonders sporadisch gesät, sofern $h \equiv 3 \mod 6$. Zum Beispiel sind für $h = 3$ nur $n \in \{3, 5\}$ und für $h = 9$ nur $n \in \{9, 15\}$ bekannt.

[1] Siehe das Literaturverzeichnis von [5] hierzu.

2 Satz von Maynard

Wir gehen auf einige bekannte Vermutungen bezüglich wiederkehrender Muster von Primzahltupeln ein.

2.1 Hardy-Littlewood'sche k-Tupel-Vermutung

Diese erste Vermutung beschäftigt sich mit wiederkehrenden Abständen von Primzahlen. Wir folgen hier der Arbeit von Maynard [9].

Definition 2.1.1. Seien $k \in \mathbb{N}$ und $T = \{h_1, \ldots, h_k\} \subset \mathbb{N}, |T| = k$, so, dass $\iota_p(T) \neq \mathbb{Z}/p\mathbb{Z}$ für alle $p \in \mathbb{P}$, wobei ι_n für $n \in \mathbb{N}$ die kanonische Projektion

$$\iota_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad z \mapsto z \mod n$$

darstellt. Dann heißt T ein *zulässiges* k-Tupel.

Wir betrachten also Tupel, die bei der ganzzahligen Division für jede Primzahl mindestens eine Restklasse nicht abdecken. Im Fall, dass es für ein k-Tupel T ein $p \in \mathbb{P}$ gibt, sodass alle Restklassen modulo p abgedeckt sind, können wir nämlich für jedes $n \in \mathbb{N}$ ein $1 \leq i \leq k$ finden, sodass $p|n + h_i$. Folglich kann $n + h_i$ dann nur prim sein, sofern es selbst p oder $-p$ ist, und widerspricht der nächsten Vermutung.

Vermutung 2.1.2. (Hardy-Littlewood) Seien $k \in \mathbb{N}$ und $T = \{h_1, \ldots, h_k\}$ ein zulässiges k-Tupel. Dann gibt es unendlich viele $n \in \mathbb{N}$, sodass $n+T = \{n+h_1, \ldots, n+h_k\}$ sämtlich aus Primzahlen besteht.

Der Spezialfall $k = 2$, $h_1 = 0$ und $h_2 = 2$ ist auch bekannt als Primzahlzwillingsvermutung. Die Hardy-Littlewood'sche Vermutung konnte bisher nicht bewiesen werden. Jedoch gab es in den vergangenen Jahren einigen Fortschritt hierzu und Maynard und Tao waren voneinander unabhängig in der Lage, eine abgeschwächte Version der Vermutung zu beweisen.

Satz 2.1.3. (Maynard-Tao) Sei $m \in \mathbb{N}$. Dann gibt es eine Konstante $k_m \in \mathbb{N}$, sodass es für alle zulässigen k-Tupel T mit $k \geq k_m$ unendlich viele $n \in \mathbb{N}$ gibt, für die mindestens m Elemente in $n + T$ prim sind.

Offensichtlich ist m eine untere Schranke für k_m. Die Hardy-Littlewood'sche Vermutung sagt uns, dass $k_m = m$ für alle m. Maynard zeigt in seiner Arbeit [9], dass $k_2 \leq 105$ gilt. Er wählt sodann ein zulässiges 105-Tupel T mit $0 = h_1 < \ldots < h_{105} = 600$ und folgert so, dass

$$\liminf_n (p_{n+1} - p_n) \leq 600,$$

wobei p_n die n-te Primzahl ist. Wir werden später sehen, dass diese Schranke noch verbessert werden konnte.

2.2 Dickson'sche Vermutung

Die Vermutung von Dickson, auch Dickson-Hardy-Littlewood'sche Vermutung genannt, verallgemeinert die Hardy-Littlewood'sche Vermutung auf lineare Formen, wozu Maynard einen Artikel [10] veröffentlichte.

Definition 2.2.1. Seien $k \in \mathbb{N}$ und $\mathcal{L} = \{l_1, \ldots, l_k\}, |\mathcal{L}| = k$, eine Menge linearer Formen aus $\mathbb{Z}[x]$, wobei $l_i = a_i x + b_i$. $\mathcal{L}$ ist ein *zulässiges* k-Tupel *linearer Formen*, falls es kein $p \in \mathbb{P}$ gibt, sodass $p| \prod_{i=1}^k l_i(n)$ für alle $n \in \mathbb{N}$.

Mit der Identifikation $h_i \mapsto x + h_i$ sehen wir, dass jedes zulässige k-Tupel auch ein zulässiges k-Tupel linearer Formen ist, da $p| \prod_{i=1}^k n + h_i$ für alle $n \in \mathbb{N}$ impliziert, dass ein Faktor von p geteilt wird und die h_i damit alle Restklassen modulo p abdecken.

Wir bezeichnen für eine Menge linearer Formen $\mathcal{L} = \{l_1, \ldots, l_k\}$ und eine Zahl $n \in \mathbb{N}$ mit $\mathcal{L}(n)$ die Menge $\{l_1(n), \ldots, l_k(n)\}$.

Vermutung 2.2.2. (Dickson) Seien $k \in \mathbb{N}$ und $\mathcal{L}$ ein zulässiges k-Tupel linearer Formen. Dann gibt es unendlich viele $n \in \mathbb{N}$, sodass alle Zahlen in $\mathcal{L}(n)$ prim sind.

Auch diese Vermutung ist bisher unbewiesen. Ein Beweis hierfür würde auch die Hardy-Littlewood'sche Vermutung beweisen, wie wir oben gesehen haben. Jedoch gibt es hierzu auch eine Teillösung von Maynard.

Satz 2.2.3. (Maynard) Sei $m \in \mathbb{N}$. Dann gibt es eine Konstante $K_m \in \mathbb{N}$, sodass es für alle zulässigen k-Tupel $\mathcal{L}$ von linearen Formen mit $k \geq K_m$ unendlich viele $n \in \mathbb{N}$ gibt, für die mindestens m Elemente in $\mathcal{L}(n)$ prim sind.

Auch wenn dieser Satz nur eine Abschwächung der Dickson'schen Vermutung ist, so können wir doch sagen, dass es in jedem k-Tupel linearer Formen mit $k \geq K_m$ Indizes $1 \leq i_1 < \ldots < i_m \leq k$ gibt, sodass folgende Hypothese für $l_{i_i}, \ldots, l_{i_m}$ gilt:

Hypothese $\mathcal{P}_m(l_{i_1}, \ldots, l_{i_m})$. Es gibt unendlich viele $n \in \mathbb{N}$, sodass $l_{i_1}(n), \ldots, l_{i_m}(n)$ gleichzeitig prim sind.

2.3 Selberg-Sieb

Das Kernstück in sämtlichen Beweisen von Maynard und darauf aufbauenden Arbeiten ([10], [9] und [1]) ist das sogenannte Selberg-Sieb. Wir schauen uns beispielhaft den Beweis für Satz 2.1.3 [9] an, da Ford [5, App. A] bemerkt, dass, da man nach Fixierung unserer Linearformen den Beweis analog durchführen kann, die Schranken für k_2 dieselben wie für K_2 sind.

Es seien $k \in \mathbb{N}$ und $T = \{h_1, \ldots, h_k\}$ ein zulässiges k-Tupel. Wir bezeichnen mit χ_A die Indikatorfunktion der Menge A. Es wird für $N \in \mathbb{N}, \rho \in \mathbb{R}_+$ die Summe

$$S(N,\rho) = \sum_{N \leq n < 2N} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n+h_i) - \rho \right) \omega_n$$

definiert, wo ω_n positive Gewichte sind, auf die wir später etwas eingehen. Dies wird aufgeteilt in

$$\begin{aligned} S_1(N,\rho) &= \sum_{N \leq n < 2N} \sum_{i=1}^{k} \chi_{\mathbb{P}}(n+h_i)\omega_n \qquad \text{und} \\ S_2(N,\rho) &= \sum_{N \leq n < 2N} \omega_n, \end{aligned}$$

sodass

$$S(N,\rho) = S_1(N,\rho) - \rho S_2(N,\rho)$$

gilt. Falls gilt, dass $S(N,\rho) > 0$ für alle großen N, können wir schließen, dass unendlich oft mindestens $\lfloor \rho + 1 \rfloor$ der Zahlen in $n + T$ prim sind.

Die Gewichte ω_n werden so gesetzt, dass sie verschwinden, sofern n nicht in einer festen Restklasse $\nu \mod W$ liegt, wobei $W = \prod_{p \leq D} p$. Dies soll einige Schwierigkeiten mit kleineren Primfaktoren beheben. Die Wahl von D wird hier als nicht wichtig gesehen, solange $W \in O((\log\log N)^2)$, sodass $D = \log\log\log N$ wegen des Primzahlsatzes ausreicht.

2.4 Qualitative Resultate für K_m

Wenngleich Maynard in seiner Arbeit [9] zeigte, dass $K_2 \leq 105$ gilt, konnte das PolyMath8b Projekt [12] diese Schranke auf $K_2 \leq 50$ verbessern.

Aus $K_2 \leq 50$ konnte in [12] mit einem passenden zulässigen 50-Tupel gezeigt werden, dass

$$\liminf_{n} \, (p_{n+1} - p_n) \leq 246$$

gilt, was eine deutliche Verbesserung gegenüber Maynards erster Schranke darstellt.

Maynard [9] zeigte außerdem, dass die Elliott-Halberstam-Vermutung $K_2 \leq 5$ impliziert und somit

$$\liminf_{n} (p_{n+1} - p_n) \leq 12$$

folgt.

Unter Annahme einer Verallgemeinerung der Elliot-Halberstam-Vermutung wurde wiederum im PolyMath8b Projekt [12] $K_2 \leq 3$ gezeigt und die Schranke so auf

$$\liminf_{n} (p_{n+1} - p_n) \leq 6$$

gesenkt.

3 Lösungen zu $\phi(n) = \phi(n+h)$ und $\sigma(n) = \sigma(n+h)$

Dieser Abschnitt bezieht sich auf den Artikel [5] von Kevin Ford, in welchem dieser teils konkrete Lösungen $h \in \mathbb{N}$ zu $\mathcal{S}_h$ gibt. Seine Arbeit hierzu wird in den ersten zwei Unterkapiteln wiedergegeben, in 3.3 befassen wir uns mithilfe Maynards Arbeit [10] mit einer unteren Schranke für die Zählfunktion $\mathcal{R}_h(n)$.

3.1 Unendlich viele Lösungen

Das Hauptresultat von Fords Arbeit ist nachstehender Satz, der uns unendlich viele Zahlen $h \in \mathbb{N}$ gibt, sodass $\mathcal{S}_h$ gilt.

Satz 3.1.1. (Ford) Es gelten die folgenden Aussagen:

1. $\mathcal{S}_h$ ist wahr für alle $h \in \mathbb{N}$ mit $\Lambda = 442720643463713815200|h$.

2. Falls $K_2 \leq 5$, dann gilt $\mathcal{S}_h$ für alle h mit $30|h$.

3. Falls $K_2 \leq 4$, dann gilt $\mathcal{S}_h$ für alle h mit $6|h$.

4. Es gibt ein gerades $l \leq 3570$, sodass $\mathcal{S}_h$ für alle h mit $l|h$ gilt.

Kernbestandteil von Fords Beweis ist Satz 2.2.3 von Maynard über zulässige k-Tupel linearer Formen und insbesondere die Folgerung der Hypothese $\mathcal{P}_m(l_{i_1}, \ldots, l_{i_m})$ für ein entsprechend gewähltes k-Tupel linearer Formen und Indizes $1 \leq i_1 < \ldots < i_m \leq k$. Des Weiteren konnte Ford zeigen, dass diese Vorgehensweise eine Aussage liefert, die noch etwas mehr an die Vermutung 1.0.2 von Erdős erinnert.

Satz 3.1.2. (Ford) Sei $m \geq 3$. Dann gibt es ein m-Tupel $\{h_1, \ldots, h_m\} \subset \mathbb{N}$, sodass für jedes $l \in \mathbb{N}$ das Gleichungssystem

$$\phi(n + lh_1) = \ldots = \phi(n + lh_m)$$

unendlich viele Lösungen $n \in \mathbb{N}$ hat.

Falls für jedes m das jeweilige m-Tupel $\{0, \ldots, m-1\}$ ist, so ist Erdős' Vermutung bewiesen.

Eine Lösung zur Hypothese $\mathcal{T}_h$ liefert Ford nicht, jedoch kann er eine zu vorhergehendem Satz ähnliche Aussage beweisen, sofern wir eine genügend große Menge an sogenannten *Freunden* finden.

Definition 3.1.3. Wir nennen eine Menge $\{a_1, \dots, a_n\}$ von n natürlichen Zahlen *Freunde*, falls für alle $1 \leq i \leq n$ stets

$$\frac{\sigma(a_i)}{a_i} = y$$

für ein festes $y \in \mathbb{Q}$ gilt.

Satz 3.1.4. (Ford) Sei $m \geq 2$ und es gebe ein Tupel $\{h_1, \dots, h_k\} \subset \mathbb{N}$ aus k Freunden mit $k \geq K_m$. Dann gibt es m positive natürliche Zahlen $d_1 < \dots < d_m$, sodass für einen positiven Anteil aller $l \in \mathbb{N}$ das Gleichungssystem

$$\sigma(n + ld_1) = \dots = \sigma(n + ld_m)$$

unendlich viele Lösungen $n \in \mathbb{N}$ hat.

Zuletzt geben wir noch ein Resultat wieder, das nur zum Teil in Fords Arbeit auftaucht, da Ford nur den ersten Satz von Korollar 3.1.6 beweist und nicht durch Einsetzung von etwaigen Tupeln auf konkrete Werte schließt. Hierfür brauchen wir die Mersenne-Primzahlen.

Definition 3.1.5. Sei $p \in \mathbb{P}$ eine Primzahl, sodass $2^p - 1$ prim ist. Dann nennen wir $2^p - 1$ eine *Mersenne*-Primzahl. Dabei sei M_i die i-te Mersenne-Primzahl und q_i ihr Exponent, sodass $M_i = 2^{q_i} - 1$.

Korollar 3.1.6. Für einen positiven Anteil aller $h \in \mathbb{N}$ gilt die Hypothese $\mathcal{T}_h$. Wir definieren

$$E_i = 2 \prod_{j=1}^{i} M_j.$$

Insbesondere gilt dann:

1. Es gibt ein $l \leq 2^{77232916}(2^{77232917} - 1) - 6$, sodass $\mathcal{T}_h$ für alle $h = bl$ mit $(b, E_{50}) = 1$ gilt.

2. Falls $K_2 \leq 5$, dann gibt es ein $l \leq 33550330$, sodass $\mathcal{T}_h$ für alle $h = bl$ mit $(b, E_5) = 1$ gilt.

3. Falls $K_2 \leq 3$, dann gibt es ein $l \leq 490$, sodass $\mathcal{T}_h$ für alle $h = bl$ mit $(b, E_3) = 1$ gilt.

3.2 Beweise zu Fords Resultaten

Zuerst legen wir für $0 < a < b \in \mathbb{N}$ folgende Definitionen fest:

$$a' = \frac{a}{(a,b)}, \quad b' = \frac{b}{(a,b)}, \quad s(a,b) = \prod_{p \mid a'b',\, p \text{ prim}} p, \quad \kappa(a,b) = (b' - a')s(a,b).$$

Wir beobachten sofort, dass $\kappa(a,b)$ immer gerade ist. Nun zäumen wir das Pferd von hinten auf.

Lemma 3.2.1. $\mathcal{P}_2(ax+1, bx+1)$ impliziert $\mathcal{S}_h$ für alle $h \in \mathbb{N}$ mit $\kappa(a,b)|h$.

Beweis. Sei $n \in \mathbb{N}$, sodass $an+1$ und $bn+1$ prim sind. Dann sind auch $a'(a,b)n+1$ und $b'(a,b)n+1$ prim und $(a,b)n \in \mathbb{N}$. Also folgt $\mathcal{P}_2(a'x+1, b'x+1)$.

Sei $l \in \mathbb{N}$ beliebig und wähle $r \in \mathbb{N}$, sodass $r > \max\{a,b,l\}$ und $a'r+1$ und $b'r+1$ prim sind. Wir definieren

$$m_1 = b'ls(a,b)(a'r+1), \qquad m_2 = a'ls(a,b)(b'r+1).$$

Dann gilt

$$m_1 - m_2 = ls(a,b)(b'-a') = l\kappa(a,b)$$

und, da die Primfaktoren von a' und b' sämtlich $s(a,b)$ teilen,

$$\begin{aligned}\phi(m_1) &= \phi(b'ls(a,b))\phi(a'r+1) = \phi(ls(a,b))b'a'r \\ &= \phi(a'ls(a,b))\phi(b'r+1) = \phi(m_2).\end{aligned}$$

Da $l \in \mathbb{N}$ beliebig war, folgt hiermit die Aussage. □

Um eine für unsere Aussagen geeignete Menge von zulässigen m-Tupeln linearer Formen zu erhalten, benutzen wir folgende technische Aussage.

Technisches Lemma 3.2.2. Eine Menge $\mathcal{L}_1 = \{l_1, \ldots, l_m\}$ von m linearen Formen der Gestalt $l_i = a_ix+1$, $1 \le i \le m$, oder $l_i = a_ix-1$, $1 \le i \le m$, mit $a_i \neq a_j$ für $i \neq j$ ist ein zulässiges m-Tupel.

Beweis. Sei $P_i^{\pm}$ die Menge der Primfaktoren von $a_i \pm 1$ und $f_\pm = \prod_{p \in P_i^{\pm}} p$. Dann ist für alle $1 \le i \le m$ stets $a_if_\pm \pm 1$ teilerfremd zu $a_j \pm 1$ für alle $1 \le j \le m$, also auch $\prod_{i=1}^m l_i(f_\pm)$ zu $\prod_{i=1}^m l_i(1)$. □

Beweis zu Satz 3.1.1. Die nächste Überlegung ist, dass wir wegen Satz 2.2.3 und der qualitativen Resultate zu K_2 [12] für zwei lineare Formen l_1, l_2 in einem zulässigen 50-Tupel auf die Hypothese $\mathcal{P}_2(l_1, l_2)$ schließen dürfen, wobei wir jedoch l_1 und l_2 nicht bestimmen können. Wenn alle Linearformen die Gestalt wie in Lemma 3.2.1 (zum Beispiel $l_1 = a_1x+1, l_2 = a_2x+1$) haben, dann können wir daraus folgern, dass $\mathcal{S}_h$ für alle Vielfachen von $\kappa(a_1, a_2)$ gilt. Da wir a_1 und a_2 nicht exakt bestimmen können, können wir die Aussage lediglich für das kleinste gemeinsame Vielfache der $\kappa(a_i, a_j)$ für $a_i < a_j$ beweisen.

Dies wenden wir nun Schritt für Schritt für die einzelnen Teile des Satzes an:

1. Passend hierfür ist das 50-Tupel

$$\begin{aligned}A_1 =\{&1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,\\&25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,\\&45,46,47,48,49,52,56\},\end{aligned}$$

   da wir nach einiger Rechnung feststellen, dass

$$\mathrm{kgV}\{\kappa(a,b) : \ a,b \in A_1,\ a<b\} = 2^5 3^3 5^2 \prod_{\substack{7\leq p\leq 47\\ p\,\mathrm{prim}}} p = \Lambda.$$

2. Dasselbe mit

$$A_2 = \{1,2,3,4,6\}$$

   und

$$\mathrm{kgV}\{\kappa(a,b) : \ a,b \in A_2,\ a<b\} = 30.$$

3. Ebenso mit

$$A_3 = \{1,2,3,4\}$$

   und

$$\mathrm{kgV}\{\kappa(a,b) : \ a,b \in A_3,\ a<b\} = 6.$$

4. Dies ist der einzige Teil, bei dem wir das Maximum und nicht das kleinste gemeinsame Vielfache der $\kappa(a,b)$ möglichst klein halten wollen. Um möglichst kleine und wenig verschiedene Primteiler zu erhalten, wählt Ford 50 relativ kleine Zahlen, deren Primteiler nur aus 2, 3 und 5 bestehen.

$$\begin{aligned}A_4 =\{&15,20,30,36,40,45,60,72,75,80,90,96,100,108,120,135,\\&144,150,180,192,200,216,225,240,250,270,288,300,320,\\&324,360,375,384,400,405,450,480,500,540,600,720,750,\\&810,900,960,1080,1200,1440,1500,1800\}\end{aligned}$$

   Hieraus ergibt sich

$$\max\{\kappa(a,b) : a,b \in A_4,\ a<b\} = 3570,$$

   woraus wir mit unserer ersten Beobachtung zusammen Teil 4 folgern. □

Im vorigen Beweis haben wir hauptsächlich darauf gebaut, dass wir die Hypothese $\mathcal{P}_2(l_1,l_2)$ für zwei lineare Formen l_1,l_2 benutzen durften. Für $m \geq 3$ ist jedoch nicht so viel über k_m beziehungsweise K_m bekannt. Nichtsdestotrotz liefert uns Satz 2.2.3 von Maynard, dass wir unsere Menge $\mathcal{L}$ von Linearformen nur groß genug wählen müssen, um die nötigen Voraussetzungen für unser Ergebnis zu erreichen.

Beweis zu Satz 3.1.2. Sei $M = \{a_1, \ldots, a_k\} \subset \mathbb{N}_+$ eine beliebige k-elementige Menge positiver Zahlen mit $k \geq K_m$. Dann gibt es Indizes $1 \leq i_1 < \ldots < i_m \leq k$ sodass $\mathcal{P}_m(a_{i_1}x + 1, \ldots, a_{i_m}x + 1)$ gilt. Nun definieren wir

$$h_j = \frac{\prod_{s=1}^m a_{i_s}^2}{a_{i_j}} \in \mathbb{N}$$

für jedes $1 \leq j \leq m$. Da $\mathcal{P}_m(a_{i_1}x + 1, \ldots, a_{i_m}x + 1)$ wahr ist, können wir für jedes $l \in \mathbb{N}$ unendlich viele $r > l$ wählen, sodass $a_{i_1}r + 1, \ldots, a_{i_m}r + 1$ gleichzeitig prim sind. Sei nun $n = lr \prod_{s=1}^m a_{i_j}^2$. Es folgt für jedes j mit den bereits angewandten Rechenregeln für die Eulerfunktion:

$$\phi(n + lh_j) = \phi(lh_j(a_{i_j}r + 1)) = \phi(lh_j)a_{i_j}r = \phi(l \prod_{s=1}^m a_{i_s}^2)r.$$

Da der letzte Term unabhängig von j ist, folgt damit die Aussage. □

Beweis zu Satz 3.1.4. Wir verfahren ähnlich wie zum vorhergehenden Beweis. Für k Freunde $\{h_1, \ldots, h_k\}$ mit $k \geq K_m$ definiere $A = \text{kgV}\{h_1, \ldots, h_k\}$ und $b_i = \frac{A}{h_i}$ für $1 \leq i \leq k$. Es sei $\frac{\sigma(h_i)}{h_i} = y$ für alle i. Wir können die Hypothese $\mathcal{P}_m(b_{i_1}x - 1, \ldots, b_{i_m}x - 1)$ für bestimmte Indizes $1 \leq i_1 < \ldots < i_m \leq k$ folgern. Dann können wir für jedes $l \in \mathbb{N}$ mit $(l, A) = 1$ unendlich viele $r > A$ finden, sodass alle $b_{i_j}r - 1$ prim sind und für

$$t_j = lh_{i_j}(b_{i_j}r - 1) = Alr - lh_{i_j}$$

stets

$$\sigma(t_j) = \sigma(l)\sigma(h_{i_j})b_{i_j}r = \sigma(l)\sigma(h_{i_j})\frac{A}{h_{i_j}}r = \sigma(l)Ayr$$

gilt. Da die zu A teilerfremden l einen positiven Anteil der natürlichen Zahlen ausmachen, ist der Beweis vollbracht. □

Beweis zu Korollar 3.1.6. Der Spezialfall $m = 2$ liefert uns unendlich viele Lösungen $n \in \mathbb{N}$ für

$$\sigma(n + lh_{i_1}) = \sigma(n + lh_{i_2}).$$

Also erhalten wir die Hypothese $\mathcal{T}_h$ für $h = l(h_{i_2} - h_{i_1})$, und da die l aus einem positiven Anteil von $\mathbb{N}$ gewählt werden können, folgt die Aussage.

Wir bedienen uns der Liste von bekannten vollkommenen Zahlen, die mittlerweile 51

Zahlen umfasst. Sie haben sämtlich die Form

$$h_i = 2^{q_i - 1} M_i$$

und erfüllen

$$\frac{\sigma(h_i)}{h_i} = 2.$$

Es gilt

$$\begin{aligned} q_1 &= 2 \\ q_{50} &\leq 77232917, \end{aligned}$$

wobei wir wissen, dass $2^{77232917} - 1$ prim ist. Folglich gibt es ein

$$l \leq h_{50} - h_1 \leq 2^{77232916}(2^{77232917} - 1) - 6,$$

sodass $\mathcal{T}_l$ gilt. Dies ist eine Schranke mit 46498849 Dezimalstellen. In Anbetracht der abschätzbaren Größe von M_{50} ist dieses Ergebnis noch relativ unerleuchtend und wir hoffen auf bessere Schranken durch die Elliott-Halberstam-Vermutung. Es sind

$$\begin{aligned} q_3 &= 5 \\ q_5 &= 13, \end{aligned}$$

also $M_3 = 31$ und $M_5 = 8191$. Dann falls $K_2 \leq 5$, folgt $\mathcal{T}_l$ für ein l mit

$$l \leq h_5 - h_1 = 4096 \cdot 8191 - 6 = 33550330,$$

und falls $K_2 \leq 3$, dann

$$l \leq h_3 - h_1 = 16 \cdot 31 - 6 = 490.$$

Die Aussage über die Vielfachen von l der Art bl mit $(b, E_j) = 1$, $j = 50, 5, 3$, erhalten wir durch die Bedingung von Satz 3.1.4, dass die Vielfachen nur durch Multiplikation mit zum kgV der M_i teilerfremden Faktoren entstehen dürfen. □

3.3 Schranken für $\mathcal{R}_h(n)$

Wir nehmen im Folgenden an, dass für $h \in \mathbb{N}$ nun $\mathcal{S}_h$ gilt. Bei einer unendlichen Anzahl von $n \in \mathbb{N}$, sodass $\phi(n) = \phi(n + h)$ gilt, stellt sich die natürliche Frage nach der Zählfunktion für diese Gleichung.

Definition 3.3.1. Sei $h \in \mathbb{N}$. Wir definieren die Zählfunktion

$$\mathcal{R}_h(n) = |\{1 \leq x \leq n : \phi(x) = \phi(x+h)\}|$$

für das Wachstum der Anzahl unserer n in der Hypothese $\mathcal{S}_h$.

Einige Arbeit hier zu haben bereits Graham, Holt und Pomerance [13] geleistet, die folgendes Resultat erhielten:

Vermutung 3.3.2. Seien $a < b$ teilerfremde natürliche Zahlen. Dann gilt

$$\sum_{\substack{r \leq n \\ ar+1 \in \mathbb{P} \\ br+1 \in \mathbb{P}}} 1 \sim 2C_2 \prod_{\substack{p \mid ab(b-a) \\ p \in \mathbb{P}_{\geq 3}}} \left(\frac{p-1}{p-2}\right) \int_2^n \frac{1}{\log at \log bt} \mathrm{d}t$$

für $n > 2$, wobei $C_2 = \prod_{p \in \mathbb{P}_{\geq 3}} (1 - \frac{1}{(p-1)^2})$ die sogenannte *Primzwilling*-Konstante ist.

Das entspricht auch unseren Erwartungen, da die Wahrscheinlichkeit, dass eine Zahl kleiner als n prim ist, $\frac{1}{\log n}$ ist. Dass zwei ausgewählte Zahlen prim sind, sollte folglich ungefähr $\frac{1}{(\log n)^2}$ sein und mit der Anzahl der Zahlen kleiner gleich n multipliziert ergibt sich $\frac{n}{(\log n)^2}$, womit man das Integral ersetzen kann, ohne die asymptotische Relation zu verletzen.

Satz 3.3.3. [13, S. 8, Corollary 1] Sei $h \in 2\mathbb{N}_+$ und

$$c(h) = \sum_{j \in P(h)} \frac{(j, j+h)}{j(j+h)} \prod_{\substack{p \in \mathbb{P}_{\geq 3} \\ p \mid \frac{jk(j+h)}{(j,j+h)^3}}} \frac{p-1}{p-2},$$

wobei $P(h) = \{p_1^{e_1} \dots p_s^{e_s} : p_i \mid h \, \forall \, i \leq s, e_i \in \mathbb{N} \, \forall \, i \leq s\}$. Dann ist $0 < c(h) < \infty$, und falls die Vermutung 3.3.2 wahr ist, gilt

$$\mathcal{R}_h(n) \sim 2C_2 c(h) \frac{n}{(\log n)^2}$$

für $n \to \infty$.

Wir wollen uns jedoch mit unbedingten Schranken beschäftigen. Es lohnt sich, zu diesem Zweck einen genaueren Blick auf Maynards Arbeit zu zulässigen linearen Formen [10] zu werfen. Da es sich hierbei um ein verallgemeinerndes Ergebnis handelt, das auch die Menge der in die Linearformen einzusetzenden Argumente und der zu erreichenden Primzahlen berücksichtigt, stellt Maynard vorher einige Voraussetzungen an eben diese

Mengen, die jedoch sämtlich von $\mathbb{N}$ als Argumentmenge und $\mathbb{P}$ als Primzahlmenge erfüllt werden.

Wir definieren

$$\pi(n) = |\{p \leq n : p \, \text{prim}\}|$$

als die Primzahlzählfunktion und

$$\pi(n; q, a) = |\{p \leq n : p \, \text{prim} \wedge p \equiv a \mod q\}|$$

für die Primzahlzählfunktion hinsichtlich einer zu $q \in \mathbb{N}$ teilerfremden Restklasse. Ähnlich dazu bezeichnen wir für ein beliebiges $n \in \mathbb{N}$ mit

$$\mathcal{A}(n) = \{x : n \leq x < 2n\}$$

und mit

$$\mathcal{A}(n; q, a) := \{n \leq x < 2n : \, n \equiv a \mod q\}$$

die Menge der modulo q zu a kongruenten x zwischen n und $2n$.

Vermutung 3.3.4. (Elliott-Halberstam) Für jedes $0 < \theta < 1$ und $A > 1$ gibt es eine Konstante $C > 0$, sodass

$$\sum_{1 \leq q \leq n^\theta} \max_{(a,q)=1} \left| \pi(n; q, a) - \frac{\pi(n)}{\phi(q)} \right| \leq \frac{Cn}{\log^A n}$$

für alle $n > 2$.

Für $\theta = 1$ ist die Aussage falsch, der Fall $0 < \theta < 1/2$ wurde im Satz von Bombieri-Vinogradov bewiesen. An die gegebenen Fakten von $\mathbb{N}$ und $\mathbb{P}$ angepasst, ergibt sich folgender Satz bei Maynard.

Satz 3.3.5. (Maynard) Es seien $n \in \mathbb{N}$, $\alpha > 0$ und $0 < \theta < 1$. Sei $k \in \mathbb{N}$ und $\mathcal{L} = \{l_1, \ldots, l_k\}, l_i = a_i x + b_i$, eine Menge von k zulässigen linearen Formen aus $\mathbb{Z}[x]$ mit positiven a_i, sodass $|a_i|, |b_i| \leq n^\alpha$ und $k \leq (\log n)^\alpha$. Es gelte:

$$\sum_{1 \leq q \leq n^\theta} \max_{(a,q)=1} \left| \pi(n; q, a) - \frac{\pi(n)}{\phi(q)} \right| \leq \frac{C_1 n}{\log^{100k^2} n}$$

und

$$\sum_{1 \leq q \leq n^\theta} \max_{(l_i(a),q)=1} \left| |l_i(\mathcal{A}(n; q, a)) \cap \mathbb{P}| - \frac{|l_i(\mathcal{A}(n)) \cap \mathbb{P}| \, \phi(|a_i|)}{\phi(|a_i| q)} \right| \leq \frac{C_2 |l_i(\mathcal{A}(n)) \cap \mathbb{P}| \, \phi(|a_1|)}{\log^{100k^2} n}$$

für bestimmte Konstanten $C_1, C_2 > 0$ und jedes $1 \le i \le k$.

Dann gibt es eine Konstante $C > 0$, die nur von α und θ abhängt, sodass das Folgende für genügend große n gilt:

Falls $k \ge C$ und es ein $\delta > (\log k)^{-1}$ gibt, sodass

$$\frac{1}{k}\sum_{i=1}^{k}\frac{\phi(a_i)}{a_i}|l_i(\mathcal{A}(n)) \cap \mathbb{P}| \ge \delta\frac{n}{\log n},$$

dann gibt es eine Konstante $D > 0$, sodass

$$|\{n \le x < 2n : |\mathcal{L}(x) \cap \mathbb{P}| \ge C^{-1}\delta \log k\}| \ge D\frac{n}{(\log n)^k \exp(Ck)}$$

gilt.

Die Bestimmung von C führt uns dann zu obigen Resultaten, sodass $C^{-1}\delta \log 50 > 1$ im Falle von $K_2 \le 50$ führt. Uns fällt auch sofort auf, dass eine untere Schranke für $|\{n \le x < 2n : |\mathcal{L}(x) \cap \mathbb{P}| \ge 2\}|$ uns auch eine untere Schranke für die Funktion $\mathcal{R}_h(n)$ liefert.

Es sei $\mathcal{L}$ wieder unsere Menge an 50 zulässigen linearen Formen, die sich durch $l_i = a_i x + 1$ für $1 \le i \le 50$ mit $a_i \in A_1$ aus dem Beweis zu Satz 3.1.1 ergibt. Wir wollen uns auf den Fall $h = g\Lambda$ für ein $g \in \mathbb{N}_+$ beschränken. Falls $|\mathcal{L}(r) \cap \mathbb{P}| \ge 2$, dann gibt es mindestens zwei Indizes $i_1 < i_2$, sodass $a_{i_1}r+1 = a'_{i_1}(a_{i_1}, a_{i_2})r+1$ und $a_{i_2}r+1 = a'_{i_2}(a_{i_1}, a_{i_2})r+1$ prim sind und damit $\tilde{r} = ls(a_{i_1}, a_{i_2})a'_{i_1}(a_{i_2}r+1)$ eine Lösung für $\phi(\tilde{r}) = \phi(\tilde{r}+l\kappa(a_{i_1}, a_{i_2}))$ ist. Wir wollen l nun so setzen, dass $l\kappa(a_{i_1}, a_{i_2}) = g\Lambda$, sodass wir Lösungen für $\phi(\tilde{r}) = \phi(\tilde{r} + g\Lambda)$ erhalten. Wir wollen also in Abhängigkeit von r die Größe von

$$\max_{1\le i_1 < i_2 \le 50} ls(a_{i_1}, a_{i_2})a'_{i_1}(a_{i_2}r + 1) = \max_{1\le i_1 < i_2 \le 50} ls(a_{i_1}, a_{i_2})a'_{i_1}a_{i_2}r + O(l)$$

abschätzen. Wir können $ls(a_{i_1}, a_{i_2}) = \frac{g\Lambda}{a'_{i_2} - a'_{i_1}}$ ersetzen. Der Fehlerterm bleibt auch nach Berücksichtigung der Bedingung $r > \max\{a', b', l\}$ durch eine nur von l abhängige Konstante C_l beschränkt und ist vernachlässigbar, da wir l fixieren. Damit vereinfacht sich dies zur Berechnung von

$$\max_{1\le i_1 < i_2 \le 50} \frac{a'_{i_1}a_{i_2}}{a'_{i_2} - a'_{i_1}} = \frac{a'_{47}a_{48}}{a'_{48} - a'_{47}} = \frac{48 \cdot 49}{49 - 48} = 2352.$$

Sobald $r > C_l$, können wir unsere Lösung $\tilde{r}$ mit $2353g\Lambda r$ nach oben abschätzen. Wir setzen für $h = g\Lambda$ dies in die Schranke von Satz 3.3.5 ein.

$$\begin{aligned}\mathcal{R}_h(n) &= |\{1 \leq x \leq n : \phi(x) = \phi(x+h)\}| \\ &\geq |\{1 \leq x \leq \frac{n}{2353h} : |\mathcal{L}(x) \cap \mathbb{P}| \geq 2\}| \\ &\geq |\{\frac{n}{4706h} \leq x \leq \frac{n}{2353h} : |\mathcal{L}(x) \cap \mathbb{P}| \geq 2\}| \\ &\geq \frac{D}{4706h \exp(50C)} \cdot \frac{n}{(\log n - \log 4706h)^{50}}.\end{aligned}$$

Ähnlich zur Bemerkung zur Vermutung 3.3.2 sollten wir hier ein Wachstum von $\frac{n}{(\log n)^{50}}$ erwarten, da unser Beweis von Satz 3.1.1 Teil 1 auf einer 50-elementigen Menge beruht. Sofern wir C und auch D effektiv berechnen, können wir damit für genügend große n eine echte untere Schranke für $\mathcal{R}_h(n)$ bestimmen.

Bisher haben wir uns nur mit unteren Schranken beschäftigt. Als erste triviale obere Schranke finden wir $\mathcal{R}_h(n) \leq n$. Darüber hinaus können wir die Schranke

$$\phi(n) > \frac{n}{e^\gamma \log\log n + \frac{3}{\log\log n}}$$

für alle $n \geq 3$ benutzen. [7] In der Gleichung sind e die Euler'sche Zahl und γ die Euler'sche Konstante. Damit entfallen für $\mathcal{R}_h$ sicherlich alle n, die

$$n - 1 < \frac{n+h}{e^\gamma \log\log(n+h) + \frac{3}{\log\log(n+h)}}$$

erfüllen, was uns eine weitere lineare Schranke liefert. Ebenso fallen alle n heraus, für die $n+h$ prim ist. Wir erhalten

$$\mathcal{R}_h \leq n - \frac{n+h}{\log(n+h)} + \frac{h}{\log h}$$

als eine bessere Schranke.

4 Übertrag auf Zahlkörper

4.1 Definitionen und vorliegende Resultate

Wir besprechen zunächst einige Definition und grundlegende Resultate über algebraische Ganzheitsringe, wie sie zum Beispiel bei Koch [8] zu finden sind.

Wir wissen, dass $\mathcal{O}_K$ nicht immer ein faktorieller Ring ist. Das Standardbeispiel hierfür ist $\mathbb{Z}[\sqrt{-5}]$, der Ganzheitsring von $\mathbb{Q}(\sqrt{-5})$, mit der uneindeutigen Zerlegung $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Jedoch ist $\mathcal{O}_K$ immer ein Dedekindring, weswegen wir für jedes Ideal eine eine eindeutige Zerlegung in Primideale haben. Da wir für ϕ und σ nicht zwischen assoziierten Elementen unterscheiden wollen, können wir also unsere Funktionen auf von einzelnen Elementen erzeugten Idealen definieren.

Satz 4.1.1. Sei K ein Zahlkörper und $\mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Dann gibt es eine eindeutige Zerlegung

$$\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$$

für Primideale $\mathfrak{p}_i$ mit $\mathfrak{p}_i \neq \mathfrak{p}_j$ für Indizes $i \neq j$ und Exponenten $e_i \in \mathbb{N}_+$.

Notation. Wir verwenden folgende Notationen und abkürzende Schreibweisen:

1. Wir bezeichnen für $\alpha \in \mathcal{O}_K$ mit $\alpha\mathcal{O}_K$ das von α erzeugte Ideal in $\mathcal{O}_K$. Sofern K aus dem Kontext klar ist, schreiben wir auch $\langle\alpha\rangle$.

2. Die Norm eines Elements $\alpha \in \mathcal{O}_L$ in einer Körpererweiterung L/K ist

$$N_{L/K}(\alpha) = \prod_{\xi \in \mathrm{Aut}(\overline{L}/K)} \xi(\alpha),$$

   wobei $\overline{L}$ die normale Hülle von L in $\mathbb{C}$ ist. Ist $K = \mathbb{Q}$ der Unterkörper, so schreiben wir abkürzend $N_L(\alpha)$.

3. Wir schreiben für ein Ideal $\mathfrak{a} \subset \mathcal{O}_K$ nun $|\mathfrak{a}| = |{}^{\mathcal{O}_K}/_{\mathfrak{a}}|$ für die Anzahl der Restklassen modulo $\mathfrak{a}$. Außerdem schreiben wir für ein Element $\alpha \in \mathcal{O}_K$ auch $|\alpha| = |\langle\alpha\rangle|$.

Wir sehen sofort, dass diese Notation Sinn ergibt, da sie große Ähnlichkeiten zur Betragsfunktion in $\mathbb{Z}$ aufweist und wir wissen, dass $|N_K(\alpha)|_{\mathbb{Z}} = |\alpha|$ für jeden Zahlkörper K gilt, wobei $|\,.\,|_{\mathbb{Z}}$ hier zur Verdeutlichung der Absolutbetrag auf $\mathbb{Z}$ ist. [11, S. 40]

Definition 4.1.2. Wir setzen für einen Zahlkörper K und $\alpha \in \mathcal{O}_K$:

1. $\phi_K(\alpha) = |({}^{\mathcal{O}_K}/_{\langle\alpha\rangle})^*|$,

2. $\sigma_K(\alpha) = \sum_{\mathfrak{b}|\langle\alpha\rangle} |\mathfrak{b}|$.

Eine andere Definition der σ_K-Funktion für $K = \mathbb{Q}(\zeta_3)$, wobei ζ_3 eine primitive dritte Einheitswurzel ist, haben bereits Parker, Rushall und Hunt [14] benutzt, um perfekte Zahlen in $\mathbb{Z}[\zeta_3]$[2] zu finden. Statt die Norm des von β, einem Teiler von $\alpha \in \mathcal{O}_K$, erzeugten Ideals zu nehmen, addieren sie stattdessen all diejengigen Teiler von α, die sie zuvor als *positiv* definiert haben. Hierdurch erhalten sie eine Funktion σ^*, die $\sigma^*(a) = \sigma(a)$ für alle $a \in \mathbb{N}$ erfüllt.

Koch liefert uns im Anschluss zur Definition der Eulerfunktion hilfreiche Aussagen, die wir so ähnlich schon von den ganzen Zahlen kennen. Außerdem können wir etwas Ähnliches über σ_K aussagen.

Satz 4.1.3. Sei K ein Zahlkörper. Dann gilt:

1. ϕ_K ist multiplikativ und endlich für jedes Ideal.
2. Für eine Zerlegung $\langle\alpha\rangle = \prod_{\substack{\mathfrak{p}|\langle\alpha\rangle \\ \mathfrak{p}\,\text{prim}}} \mathfrak{p}^{e_\mathfrak{p}}$ gilt $\phi_K(\alpha) = \prod_{\substack{\mathfrak{p}|\langle\alpha\rangle \\ \mathfrak{p}\,\text{prim}}} |\mathfrak{p}|^{e_\mathfrak{p}-1}(|\mathfrak{p}|-1)$.
3. Falls für jedes Primideal $\mathfrak{p} \subset \mathcal{O}_K$ aus $\mathfrak{p} \mid \mathfrak{a}$ stets $\mathfrak{p} \mid \mathfrak{b}$ für Ideale $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ folgt, dann $\phi_K(\mathfrak{a}\mathfrak{b}) = |\mathfrak{a}|\phi_K(\mathfrak{b})$.
4. σ_K ist multiplikativ und endlich für jedes Ideal.

Beweis.

1. Es seien $\mathfrak{a}, \mathfrak{b}$ teilerfremde Ideale in $\mathcal{O}_K$. Also sind $|\mathfrak{a}|$ und $|\mathfrak{b}|$ teilerfremd in $\mathbb{Z}$. Dann gilt mit dem Chinesischen Restsatz

$$\begin{aligned}\phi_K(\mathfrak{a}\mathfrak{b}) &= |(\mathcal{O}_K/\mathfrak{a}\mathfrak{b})^*| = |(\mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b})^*| = |(\mathcal{O}_K/\mathfrak{a})^* \times (\mathcal{O}_K/\mathfrak{b})^*| \\ &= |(\mathcal{O}_K/\mathfrak{a})^*| \cdot |(\mathcal{O}_K/\mathfrak{b})^*| = \phi_K(\mathfrak{a})\phi_K(\mathfrak{b}).\end{aligned}$$

Da $|(\mathcal{O}_K/\mathfrak{a})^*| < |\mathfrak{a}| < \infty$, folgt die Aussage.

2. Wegen Punkt 1 müssen wir uns die Funktion nur auf Potenzen von Primidealen, die nicht $\{0\}$ sind, ansehen. Sei $\mathfrak{p} \neq \{0\}$ prim in $\mathcal{O}_K$. Die Gleichung $\phi_K(\mathfrak{p}) = |\mathfrak{p}| - 1$ ist offensichtlich, da $\mathfrak{p}$ prim und $\mathcal{O}_K$ eindimensional ist und folglich $\mathcal{O}_K/\mathfrak{p}$ ein Körper sein muss. Wir betrachten dann die kanonische Projektion

$$\pi_n : \mathcal{O}_K/\mathfrak{p}^n \to \mathcal{O}_K/\mathfrak{p}.$$

[2] auch bekannt als Eisensteinzahlen

Es ist $\pi_n^{-1}((\mathcal{O}_K/\mathfrak{p})^*) = (\mathcal{O}_K/\mathfrak{p}^n)^*$. Damit ergibt sich die Formel, da π_n surjektiv ist und der Kern $|\mathfrak{p}|^{n-1}$ Elemente enthält.

3. Dies folgt direkt aus der Formel in Punkt 2 und der Multiplikativität der Norm und des Betrags.

4. Seien $\mathfrak{a}_1, \mathfrak{a}_2$ zwei teilerfremde Ideale in $\mathcal{O}_K$. Für eine Zerlegung $\mathfrak{b}\mathfrak{c} = \mathfrak{a}_1\mathfrak{a}_2$ gibt es deswegen eine Zerlegung in teilerfremde Paare $\mathfrak{b}_1, \mathfrak{b}_2$ und $\mathfrak{c}_1, \mathfrak{c}_2$, sodass $\mathfrak{c} = \mathfrak{c}_1\mathfrak{c}_2$ und $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ sowie $\mathfrak{a}_i = \mathfrak{b}_i\mathfrak{c}_i$ für $i = 1, 2$. Dann gilt

$$\begin{aligned}
\sigma_K(\mathfrak{a}_1\mathfrak{a}_2) &= \sum_{\mathfrak{b}\mathfrak{c}=\mathfrak{a}_1\mathfrak{a}_2} |\mathfrak{b}| \\
&= \sum_{\mathfrak{a}_i=\mathfrak{b}_i\mathfrak{c}_i} |\mathfrak{b}_1\mathfrak{b}_2| \\
&= \sum_{\mathfrak{a}_i=\mathfrak{b}_i\mathfrak{c}_i} |\mathfrak{b}_1|\,|\mathfrak{b}_2| \\
&= \sum_{\mathfrak{a}_1=\mathfrak{b}_1\mathfrak{c}_1} |\mathfrak{b}_1| \sum_{\mathfrak{a}_2=\mathfrak{b}_2\mathfrak{c}_2} |\mathfrak{b}_2| \\
&= \sigma_K(\mathfrak{a}_1)\sigma_K(\mathfrak{a}_2).
\end{aligned}$$

Damit folgt die Aussage, da jedes Ideal nach Satz 4.1.1 nur endlich viele Teiler mit auch endlicher Norm hat. □

Mittels dieser Ergebnisse können wir gut mit ϕ_K umgehen. Um uns an Fords Vorgehen zu orientieren, können wir auch noch eine Arbeit von Castillo et al. [1] heranziehen, die uns Aussagen über eine Verallgemeinerung der Hardy-Littlewood'schen k-Tupel-Vermutung über Zahlkörper bereitstellt. Hierfür müssen wir jedoch erst einmal unsere Definition von zulässigen k-Tupeln anpassen.

Definition 4.1.4. Seien K ein Zahlkörper, $k \in \mathbb{N}$ und $T = \{h_1, \ldots, h_k\} \subset \mathcal{O}_K$, $|T| = k$, so, dass $\iota_\mathfrak{p}(T) \neq \mathcal{O}_K/\mathfrak{p}$ für alle Primideale $\mathfrak{p} \subset \mathcal{O}_K$, wobei $\iota_\mathfrak{a}$ für ein Ideal $\mathfrak{a} \subset \mathcal{O}_K$ die kanonische Projektion

$$\iota_\mathfrak{a} : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}, \qquad z \mapsto z \mod \mathfrak{a}$$

darstellt. Dann heißt T ein *zulässiges* k-Tupel in K.

Castillo et al. geben uns eine einfache Möglichkeit, um schnell zulässige k-Tupel zu finden.

Lemma 4.1.5. Seien $k \in \mathbb{N}$ und T ein zulässiges k-Tupel in einem Zahlkörper K. Dann ist T zulässig in jedem Zahlkörper $L \supset K$.

Beweis. Sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}_L$. Dann gibt es ein Primideal $\mathfrak{p} \subset \mathcal{O}_K$, sodass $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Also gilt für zwei Elemente $a_1, a_2 \in \mathcal{O}_K$ stets $a_1 - a_2 \in \mathfrak{p} \Leftrightarrow a_1 - a_2 \in \mathfrak{P}$. Sei $a \in \mathcal{O}_K$ ein Repräsentant einer Restklasse, sodass es kein $h \in T$ gibt mit $\iota_{\mathfrak{p}}(h) = \iota_{\mathfrak{p}}(a)$. Also gilt für alle $h \in T$, dass $h - a \notin \mathfrak{p}$. Da aber $h, a \in \mathcal{O}_K$, folgt, dass es kein h gibt, sodass $h - a \in \mathfrak{P}$. □

Dieses Resultat lässt sich insbesondere für $K = \mathbb{Q}$ sehr gut verwenden, da L dann ein beliebiger Zahlkörper sein kann. In [1] zeigen Castillo et al., dass wir dann auch eine äquivalente Aussage zum Satz von Maynard-Tao (Satz 2.1.3) über jeden Zahlkörper erhalten.

Satz 4.1.6. (Castillo, Hall, Oliver, Pollack, Thompson) Sei K ein Zahlkörper und $m \in \mathbb{N}$. Dann gibt es einen Konstante $k_{m,K} \in \mathbb{N}$, sodass es für alle zulässigen k-Tupel T in K mit $k \geq k_{m,K}$ unendlich viele $\alpha \in \mathcal{O}_K$ gibt, für die mindestens m Elemente in $\alpha + T$ prim sind.

Castillo et al. führen aus, dass die Rechnungen zu $k_{m,K}$ denen zu $k_{m,\mathbb{Q}}$ genau entsprächen, sofern K in $\mathbb{R}$ eingebettet werden kann. Im Allgemeinen hänge $k_{m,K}$ von der Anzahl komplexer Automorphismen von K ab. Wir wollen mit [10] die äquivalente Aussage für zulässige k-Tupel linearer Formen in K benutzen, wobei wir folgende Definition verwenden.

Definition 4.1.7. Seien K ein Zahlkörper, $k \in \mathbb{N}$ und $\mathcal{L} = \{l_1, \ldots, l_k\}, |\mathcal{L}| = k$, eine Menge linearer Formen aus $\mathcal{O}_K[x]$, wobei $l_i = a_i x + b_i$. Wir nennen $\mathcal{L}$ ein *zulässiges* k-*Tupel linearer Formen in* K, falls es kein Primideal $\mathfrak{p} \subset \mathcal{O}_K$ gibt, sodass

$$\mathfrak{p} \supset \prod_{i=1}^{k} \langle l_i(\alpha) \rangle$$

für alle $\alpha \in \mathcal{O}_K$ gilt.

Wir sehen, dass wir über die Identifikation $h_1 \mapsto x + h_1$ wieder analog zur Definition in $\mathbb{Z}$ ein zulässiges k-Tupel in K immer auch als zulässiges k-Tupel linearer Formen in K betrachten können. Nun wollen wir auch Lemma 4.1.5 übertragen.

Lemma 4.1.8. Seien $k \in \mathbb{N}$ und $\mathcal{L}$ ein zulässiges k-Tupel linearer Formen in einem Zahlkörper K. Dann ist $\mathcal{L}$ zulässig in jedem Zahlkörper $L \supset K$.

Beweis. Sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}_L$. Dann gibt es ein Primideal $\mathfrak{p} \subset \mathcal{O}_K$, sodass

$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Da $\mathcal{L}$ zulässig in K ist, gibt es ein $\alpha \in \mathcal{O}_K$, sodass

$$\mathfrak{p} \not\supset \prod_{l \in \mathcal{L}} l(\alpha)\mathcal{O}_K.$$

Angenommen, dass $\mathfrak{P} \supset \prod_{l\in\mathcal{L}} l(\alpha)\mathcal{O}_L$. Dann würde folgen, dass

$$\prod_{l \in \mathcal{L}} l(\alpha)\mathcal{O}_K \subset \prod_{l \in \mathcal{L}} l(\alpha)\mathcal{O}_L \cap \mathcal{O}_K \subset \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}.$$

Dies ist ein Widerspruch, also gilt $\mathfrak{P} \not\supset \prod_{l\in\mathcal{L}} l(\alpha)\mathcal{O}_L$. □

Wir werden später sehen, dass die zu 4.1.6 analoge Aussage über zulässige Linearformen über einem Zahlkörper K nicht stark genug ist, um uns Lösungen für unsere Hypothesen zu liefern.

4.2 Weitere Überlegungen zu allgemeinen Zahlkörpern

Wir können Lösungen von $\phi(n) = \phi(n+h)$ nicht direkt auf einen Zahlkörper K übertragen. Dies sieht man am Beispiel $K = \mathbb{Q}(i)$ mit $\mathcal{O}_K = \mathbb{Z}[i]$, letzterer Ring ist auch bekannt als Gauß'sche Zahlen. Wir wissen, dass die Primideale in $\mathbb{Z}[i]$ folgende Form haben:

1. $\langle 1+i \rangle$,
2. $\langle p \rangle$ mit $p \in \mathbb{Z}$ und $p \equiv 3 \mod 4\mathbb{Z}$,
3. $\langle a+bi \rangle$ und $\langle a-bi \rangle$ für eine Lösung $(a,b) \in \mathbb{Z}^2$ von $a^2+b^2 = p$ für $p \in \mathbb{P}$ und $p \equiv 1 \mod 4\mathbb{Z}$. [6, S. 284]

Es gilt

$$\phi(5) = 4 = \phi(8),$$

aber

$$\phi_K(5) = \phi(2-i)\phi_K(2+i) = 4^2 = 16 \neq 32 = 2^5 = |1+i|^5\phi_K(1+i) = \phi_K(8).$$

Andererseits gilt

$$\phi_K(13) = \phi_K(3+2i)\phi_K(3-2i) = 12^2 = 72 \cdot 2 = \phi_K(9)\phi_K(2) = \phi_K(18),$$

aber

$$\phi(13) = 12 \neq 6 = \phi(18).$$

Die $h \in \mathbb{Z}$, für die $\mathcal{S}_{h,\mathbb{Q}}$ gilt, sagen uns also nicht so viel über Lösungen in anderen Zahlkörpern. Wenn wir unseren Blick jedoch auf die Wert von $\phi_K(p)$ mit $p \equiv 1 \mod 4\mathbb{Z}$

im obigen Fall richten, so erkennen wir schnell einfache Lösungen für $\mathcal{S}_{h,K}$ in Abhängigkeit von K.

Satz 4.2.1. Sei K ein Zahlkörper und G die Automorphismusgruppe von $K/\mathbb{Q}$. Seien $\xi_1, \xi_2 \in G$ beliebig und

$$h = \xi_2(\alpha) - \xi_1(\alpha)$$

für ein $\alpha \in \mathcal{O}_K$. Dann sind $\mathcal{S}_{h,K}$ und $\mathcal{T}_{h,K}$ wie auf Seite 3 definiert wahr.

Beweis. Da G eine Gruppe ist und unsere Automorphismen ξ_1, ξ_2 beliebig sind, können wir ohne Beschränkung der Allgemeinheit annehmen, dass ξ_1 die Identität ist. Ansonsten wähle $\alpha' = \xi_1(\alpha)$ und $\xi_2(\xi_1^{-1}(\alpha')) = \xi_2'(\alpha')$ und betrachte $h = \xi_2'(\alpha') - \alpha'$.

Sei $l \in \mathbb{Z}$. Aus unserer Definition der Norm folgern wir, da $\xi(l) = l$ für jedes $\xi \in G$, dass $N_K(\alpha + l) = N_K(\xi_2(\alpha + l))$, also auch $|\alpha + l| = |\xi_2(\alpha + l)| < \infty$. Sei

$$\psi : \mathcal{O}_K/\langle\alpha+l\rangle \to \mathcal{O}_K/\langle\xi_2(\alpha+l)\rangle, \qquad z \mod \langle\alpha + l\rangle \mapsto \xi_2(z) \mod \langle\xi_2(\alpha + l)\rangle.$$

Da ξ_2 ein Automorphismus ist, sehen wir, dass ψ ein Homomorphismus ist. Sei $\xi_2(z) \equiv 0 \mod \langle\xi_2(\alpha + l)\rangle$, also $\xi_2(z) = \xi_2(\alpha + l)\beta$ für ein $\beta \in \mathcal{O}_K$. Da ξ_2 ein Automorphismus ist, gibt es genau ein $\gamma \in \mathcal{O}_K$, sodass $\xi_2(\gamma) = \beta$. Dann ist $z = \xi_2^{-1}(\xi_2((\alpha + l)\gamma)) = (\alpha + l)\gamma$, also $z \equiv 0 \mod \langle\alpha + l\rangle$. Damit ist ψ injektiv und bijektiv, also ein Isomorphismus. Dies zeigt $\phi_K(\alpha + l) = \phi_K(\alpha + l + h)$. Da l beliebig war, folgt $\mathcal{S}_{h,K}$.

Da ψ ein Isomorphismus ist, können wir folgern, dass ξ_2 eine Zerlegung $\langle\alpha + l\rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ in Primideale $\mathfrak{p}_i, 1 \le i \le r$ mit $e_i, r \in \mathbb{N}_+$ bijektiv auf eine Zerlegung $\langle\xi_2(\alpha+l)\rangle = \xi_2(\mathfrak{p}_1)^{e_1} \dots \xi_2(\mathfrak{p}_r)^{e_r}$ abbildet. Dies impliziert $\mathcal{T}_{h,K}$. □

Da wir hier isomorphe Quotientenringe für die Ideale $\langle\alpha\rangle$ und $\langle\alpha + h\rangle$ und für $K = \mathbb{Q}$ sogar einfach nur $h = 0$ erhalten, können wir diese Lösungen als triviale Lösungen betrachten. Um wie Ford [5] vorzugehen und auf diese Weise eventuell nicht-triviale Lösungen zu erhalten, müssen wir aber noch einiges in seinem Beweis an die Gegebenheiten in $\mathcal{O}_K$ angleichen.

1. $\mathcal{O}_K$ ist nicht immer faktoriell. Wir können zwar wegen Lemma 4.1.8 dieselben linearen Formen benutzen, sofern die a_i in unseren $l_i = a_i x + 1$ aus $\mathbb{Z}$ gewählt werden. Jedoch können wir nicht wie in Unterkapitel 3.2

$$a' = \frac{a}{(a,b)}, \qquad b' = \frac{b}{(a,b)}$$

verwenden. Wir werden stattdessen auf das allgemeinere, aber eben in $\mathbb{Z}$ normalerweise größere

$$(\alpha - \beta)\alpha\beta \qquad \alpha, \beta \in \mathcal{O}_K$$

statt $s(a, b)$ zurückgreifen.

2. Von essentieller Bedeutung in Fords Findung von Lösungen ist die Gleichung

$$\phi(ar + 1)b = abr = \phi(br + 1)a,$$

welche aber wegen $\phi_K(ar+1) \neq |ar|$ in einem allgemeinen Zahlkörper K schwieriger zu erfüllen ist. Konkret wollen wir nun

$$\phi_K(\alpha r + 1)|\beta| = \phi_K(\beta r + 1)|\alpha| \tag{1}$$

für $\alpha, \beta \in \mathcal{O}_K$ lösen.

Für Satz 3.1.2 müssen wir diese Voraussetzungen nur linear mit m erweitern. Wir brauchen also unendlich viele $r \in \mathcal{O}_K$ mit primen $\alpha_1 r + 1, \ldots, \alpha_m r + 1$ und

$$c|\alpha_i r| = \phi_K(\alpha_i r + 1) \tag{2}$$

für ein $c \in \mathbb{Q}$.

3. Bei der σ-Funktion müssen wir dasselbe wie für Satz 3.1.2 beachten, da dort ein ähnliches Schema benutzt wurde. Jedoch haben wir dort schon die Bedingung, dass die a_i Freunde sein sollen, welche wir nun durch eine spezifischere in $\mathcal{O}_K$ ersetzen wollen. Definiere

$$A = \prod_{i=1}^{m} \alpha_i, \qquad \beta_j = \frac{A}{\alpha_j}$$

für $1 \leq j \leq m$. Dann wollen wir zusätzlich dazu, dass unsere α_i Freunde bezüglich der σ_K-Funktion sind, auch

$$\sigma_K(\beta_i r - 1) = c|\beta_i r|$$

für alle $1 \leq i \leq m$ und ein $c \in \mathbb{Q}$.

Wir wollen dies nochmal formal aufschreiben.

Satz 4.2.2. Es sei $K/\mathbb{Q}$ eine algebraische Zahlkörpererweiterung.

1. Es seien $\alpha, \beta \in \mathcal{O}_K$, sodass es unendlich viele $r \in \mathcal{O}_K$ gibt, sodass $\alpha r + 1$ und $\beta r + 1$ gleichzeitig prim sind und (1) gilt. Dann ist $\mathcal{S}_{h,K}$ wahr für alle $h \in \mathcal{O}_K$ mit $(\alpha - \beta)\alpha\beta \mid h$.

2. Es seien $m \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$, sodass es unendlich viele $r \in \mathcal{O}_K$, sodass alle

$a_i r + 1, 1 \leq i \leq m$ gleichzeitig prim sind und (2) für ein $c \in \mathbb{Q}$ gilt. Setze

$$h_j = \alpha_j \prod_{i \neq j} \alpha_i^2$$

für alle $1 \leq j \leq m$ und wähle $l \in \mathcal{O}_K$ beliebig. Dann gibt es unendlich viele $\gamma \in \mathcal{O}_K$, sodass

$$\phi_K(\gamma + lh_1) = \ldots = \phi_K(\gamma + lh_m).$$

3. Seien $m \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$ mit $\frac{\sigma_K(\alpha_i)}{|\alpha_i|} = y$ für alle $1 \leq i \leq m$ und ein $y \in \mathbb{Q}$. Definiere

$$A = \prod_{i=1}^{m} \alpha_i, \qquad \beta_j = \frac{A}{\alpha_j}$$

für $1 \leq j \leq m$. Falls es unendlich viele $r \in \mathcal{O}_K$ gibt, sodass $\beta_1 r - 1, \ldots, \beta_m r - 1$ gleichzeitig prim sind, und

$$\sigma_K(\beta_i r - 1) = c|\beta_i r|$$

für alle $1 \leq i \leq m$ und ein $c \in \mathbb{Q}$ gilt, so gibt es für einen positiven Anteil aller $l \in \mathcal{O}_K$ unendlich viele $\gamma \in \mathcal{O}_K$, sodass

$$\sigma_K(\gamma + l\alpha_1) = \ldots = \sigma_K(\gamma + l\alpha_m)$$

wahr ist.

Beweis. Wir halten uns dicht an die Beweise aus Unterkapitel 3.2.

1. Sei $l \in \mathcal{O}_K$ beliebig und setze

$$m_1 = (\alpha r + 1)\alpha\beta^2 l, \qquad m_2 = (\beta r + 1)\alpha^2\beta l,$$

mit $|r| > \max\{|\alpha|, |\beta|, |l|\}$. Dann gilt

$$m_2 - m_1 = (\alpha - \beta)\alpha\beta l$$

und

$$\begin{aligned}
\phi_K(m_1) = \phi_K((\alpha r + 1)\alpha\beta^2 l) &= \phi_K(\alpha\beta^2 l)\phi_K(\alpha r + 1) \\
&= \phi_K(\alpha\beta l)|\beta|\phi_K(\alpha r + 1) = \phi_K(\alpha\beta l)|\alpha|\phi_K(\beta r + 1) \\
&= \phi_K((\beta r + 1)\alpha^2\beta l) = \phi_K(m_2).
\end{aligned}$$

Da es unendlich viele solche r gibt, folgt die Aussage.

2. Sei $l \in \mathcal{O}_K$ wieder beliebig und sei $r \in \mathcal{O}_K$ so, dass $\alpha_1 r + 1, \ldots, \alpha_m r + 1$ alle prim

sind und $|r| > \max\{|\alpha_1|, \ldots, |\alpha_m|, |l|\}$. Nun setze $\gamma = lr \prod_{i=1}^m \alpha_i^2$. Dann folgt wie im Beweis zu 3.1.2 für alle $1 \leq j \leq m$, dass

$$\phi_K(\gamma + lh_j) = \phi_K(lh_j(\alpha_j r + 1)) = \phi_K(lh_j)|\alpha_j r|c = \phi_K(l \prod_{i=1}^m \alpha_m^2)|r|c.$$

Da der letzte Term unabhängig von j ist, folgt wieder die Aussage.

3. Es sei wieder $l \in \mathcal{O}_K$ beliebig. Sei nun $r \in \mathcal{O}_K$, sodass $\beta_1 r - 1, \ldots, \beta_m r - 1$ prim sind und $|r| > \max\{|\beta_1|, \ldots, |\beta_m|, |l|\}$. Dann gilt wie im Beweis zu Satz 3.1.3 für alle $1 \leq j \leq m$ und $l \in \mathcal{O}_K$ mit $\langle l, A \rangle = \mathcal{O}_K$, dass

$$\begin{aligned} \sigma_K(lAr - l\alpha_j) &= \sigma_K(l\alpha_j(\beta_j r - 1) = \sigma_K(l)\sigma_K(\alpha_j)c|\beta_j r| \\ &= \sigma_K(l)|Ar|yc. \end{aligned}$$

Da die zu A teilerfremden l wieder einen positiven Anteil im Ganzheitsring ausmachen, ist die Aussage bewiesen. □

Da wir ϕ_K dank Satz 4.1.3 gut ausrechnen können, werden wir in diesem Fall auch einigen Fortschritt hinsichtlich der Erfüllung der Voraussetzungen in 4.2.2 finden. Dies ist jedoch leider für σ_K nicht der Fall, weswegen wir uns hier auf die trivialen Lösungen beschränken wollen. Außerdem haben wir bereits gesehen, dass die von Ford benutzen Linearformen $\alpha r + 1$ uns nicht immer zum Ziel führen und wir auch auf anderem Wege dorthin gelangen.

5 Lösungen in quadratischen Erweiterungen

Sei $K/\mathbb{Q}$ in diesem Kapitel stets eine quadratische Körpererweiterung. Nach Koch [8] können wir ein quadratfreies $d \in \mathbb{Z}$ finden, sodass $K = \mathbb{Q}(\sqrt{d})$. Auch die Automorphismusgruppe G von K kennen wir, es ist $G = \{\mathrm{id}, \xi\}$, wobei

$$\xi : K \to K, \qquad a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

Dies lässt uns die Norm schnell berechnen

$$N_K(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$$

Mit Satz 4.2.1 schließen wir direkt, dass $\mathcal{S}_{h,K}$ und $\mathcal{T}_{h,K}$ für alle

$$h = a - b\sqrt{d} - (a + b\sqrt{d}) = -2b\sqrt{d} \in \mathcal{O}_K$$

gilt. Wir wissen auch, wie der Ganzheitsring $\mathcal{O}_K$ aussieht.

1. $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ falls $d \equiv 2, 3 \mod 4\mathbb{Z}$ oder
2. $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ falls $d \equiv 1 \mod 4\mathbb{Z}$.

Durch Einsetzung erhalten wir, dass $\mathcal{S}_{h,K}$ und $\mathcal{T}_{h,K}$ für alle

1. $h = b\sqrt{d}$ mit $b \in 2\mathbb{Z}$ falls $d \equiv 2, 3 \mod 4\mathbb{Z}$ und
2. $h = b\sqrt{d}$ mit $b \in \mathbb{Z}$ falls $d \equiv 1 \mod 4\mathbb{Z}$

wahr sind.

Da wir uns in diesem Kapitel mit konkreten Beispielen beschäftigen wollen, werden wir folgenden Satz vereinzelt benutzen, der uns die Form aller Primideale in $\mathcal{O}_K$ errechnen lässt, da für jedes prime $\mathfrak{P} \subset \mathcal{O}_K$ es ein primes $\mathfrak{p} \subset \mathbb{Z}$ gibt, sodass $\mathfrak{P} \cap \mathbb{Z} = \mathfrak{p}$.

Satz 5.0.1. (Dedekind-Kummer) [11, S. 46] Sei $K = \mathbb{Q}(\alpha)$ ein Zahlkörper und $p \in \mathbb{P}$, sodass $p \nmid [\,\mathcal{O}_K : \mathbb{Z}[\alpha]\,]$. Sei $f \in \mathbb{Z}[x]$ das Minimalpolynom von α und $\overline{f} \equiv f \mod p$. Es sei

$$\overline{f} = \overline{f}_1^{e_1} \dots \overline{f}_r^{e_r}$$

für ein $r \in \mathbb{N}$ die Zerlegung von $\overline{f}$ in paarweise verschiedene, monische, irreduzible Polynome in $\mathbb{F}_p[x]$. Wähle für jedes i ein $f_i \in \mathbb{Z}[x]$, sodass $\overline{f}_i \equiv f_i \mod p$, und bezeichne mit $\mathfrak{p}_i$ das Ideal $\langle p, f_i(\alpha)\rangle \subset \mathcal{O}_K$. Dann gilt

$$\langle p \rangle = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

in $\mathcal{O}_K$ und $|\mathfrak{p}_i| = p^{\deg f_i}$.

In quadratischen Erweiterungen bedeutet dies, dass jedes Primideal entweder von einem Element in $\mathbb{P}$ erzeugt wird und Norm p^2 hat oder mindestens einen Erzeuger besitzt, der nicht in $\mathbb{Z}$ liegt, und Norm p hat. Wie oben beschrieben, können wir leicht ein α bestimmen, sodass $\mathcal{O}_K = \mathbb{Z}[\alpha]$ und die Bedingung somit für alle $p \in \mathbb{P}$ erfüllt ist. Für uns entscheidend ist hier, ob $\mathfrak{p}_i$ ein Hauptideal ist. Genau dann ist nämlich dessen Erzeuger prim in $\mathcal{O}_K$.

5.1 Komplexe Erweiterungen

Im Falle $d < 0$ gilt, dass K keine reelle Einbettung besitzt, und wir nennen K eine komplexe Erweiterung. Damit ist für jedes $a, b \in \mathbb{Q}$

$$N_K(a + b\sqrt{d}) = a^2 - b^2 d \geq 0$$

und konsequent

$$N_K(a + b\sqrt{d}) = |a + b\sqrt{d}|.$$

Damit können wir $|\alpha|\phi_K(\beta r + 1)$ berechnen, sofern $\beta r + 1$ prim ist. Wir benutzen, dass $\xi(1) = 1$ und $N_K(\alpha), N_K(\beta r + 1) > 0$.

$$\begin{aligned}
|\alpha|\phi_K(\beta r + 1) &= |\alpha|(|\beta r + 1| - 1) \\
&= \alpha\xi(\alpha)(\beta r\xi(\beta r) + \beta r + \xi(\beta r) + 1 - 1) \\
&= \alpha\xi(\alpha)(\beta r\xi(\beta r) + \beta r + \xi(\beta r))
\end{aligned}$$

Für $\gamma \in \mathcal{O}_K$ bezeichnen wir mit $\mathrm{rat}(\gamma)$ den rationalen Teil von $\gamma = \mathrm{rat}(\gamma) + \mathrm{irr}(\gamma)$, wobei $\mathrm{rat}(\gamma) \in \mathbb{Z}$ und $\mathrm{irr}(\gamma) \in \mathcal{O}_K \setminus \mathbb{Z}$, und definieren

$$D(\alpha, \beta, r) := |\alpha|\phi_K(\beta r + 1) - |\beta|\phi_K(\alpha r + 1).$$

Es gilt also (1) genau dann, wenn $D(\alpha, \beta, r) = 0$. Falls sowohl $\beta r + 1$ als auch $\alpha r + 1$ prim sind, können wir $D(\alpha, \beta, r)$ gut ausrechnen.

$$\begin{aligned}
D(\alpha, \beta, r) &= \alpha\xi(\alpha)(\beta r\xi(\beta r) + \beta r + \xi(\beta r)) \\
&\quad - \beta\xi(\beta)(\alpha r\xi(\alpha r) + \alpha r + \xi(\alpha r)) \\
&= \alpha\xi(\alpha)(\beta r + \xi(\beta r)) - \beta\xi(\beta)(\alpha r + \xi(\alpha r)) \\
&= \xi(\alpha - \beta)\alpha\beta r + (\alpha - \beta)\xi(\alpha\beta r) \\
&= 2\mathrm{rat}((\alpha - \beta)\alpha\beta r)
\end{aligned}$$

Dies ist 0, sofern $2(\alpha - \beta)\alpha\beta r \in \sqrt{d}\mathbb{Z}$. Da $(\alpha - \beta)\alpha\beta$ konstant ist und wir die Multiplikation in den Polarkoordinaten heranziehen können, sehen wir, dass die Bilder derjenigen r, die $D(\alpha, \beta, r)$ verschwinden lassen, unter einer Einbettung von K in $\mathbb{C}$ auf einer reellen Geraden liegen. Auch wenn Satz 4.1.6 über die Hardy-Littlewood'sche Vermutung in Zahlkörpern sich nicht auf generalisierte lineare Formen bezieht, so sehen wir bereits dort, dass die zusätzliche Forderung an die r, auf einer Geraden zu liegen, dazu führen kann, dass wir nicht unendlich viele solche r finden, sodass $\alpha r + 1$ und $\beta r + 1$ gleichzeitig prim sind.

Wenn wir mittels Lemma 4.1.8 ein Tupel zulässiger linearer Formen aus $\mathbb{Z}[x]$ wählen, müssen wir hier $r \in \sqrt{d}\mathbb{Z}$ haben, damit $(\alpha - \beta)\alpha\beta r \in \sqrt{d}\mathbb{Z}$. Nach Satz 5.0.1 ist dann ein äquivalentes Kriterium, damit $\alpha r + 1$ und $\beta r + 1$ unendlich oft gleichzeitig prim sind, dass es unendlich viele $e \in \mathbb{Z}$ gibt, sodass für $r = e\sqrt{d}$ sowohl

$$N_K(1 + \alpha e\sqrt{d}) = 1 - (\alpha e)^2 d \quad \text{als auch} \quad N_K(1 + \beta e\sqrt{d}) = 1 - (\beta e)^2 d \tag{3}$$

prim in $\mathbb{Z}$ sind. Man bemerke, dass dies über $\mathbb{Z}$ irreduzible Polynome in der Variablen e sind, da d quadratfrei ist. Dies ist eine allgemeinere Version des ersten Landau-Problems [6, S. 23] beziehungsweise von Schinzels Vermutung [4], die gleichzeitig für zwei verschiedene Koeffizienten gelten soll. Da jenes Problem aber selbst noch nicht gelöst wurde, ist es nicht wahrscheinlich, auf diesem Wege eine bedingungslose Lösung zu finden.

Vermutung 5.1.1. (Schinzel) Es sei $k \in \mathbb{N}$ und $f_1, \ldots, f_k$ eine Menge von irreduziblen Polynomen in $\mathbb{Z}[x]$, sodass für jedes $p \in \mathbb{P}$ ein $n_p \in \mathbb{N}$ mit $p \nmid \prod_{i=1}^k f_i(n_p)$ existiert. Dann gibt es unendlich viele $n \in \mathbb{N}$, sodass $f_1(n), \ldots, f_k(n)$ sämtlich prim sind.

Wir sehen, dass Schinzels Vermutung natürlich wegen Satz 4.2.2 etwas zu stark ist, da wir ähnlich wie Ford auf die $\mathcal{S}_{h,K}$ für $h = \mathrm{kgV}\{(\alpha - \beta)\alpha\beta : \alpha, \beta \in M\}$ für eine beliebige Menge M schließen können. Uns würde eine lediglich zu 2.1.3 oder 2.2.3 analoge Aussage genügen.

Vermutung 5.1.2. Sei $m \in \mathbb{N}$. Es gibt eine Konstante $\mathcal{K}_m \in \mathbb{N}$, sodass für alle $k \in \mathbb{N}$ mit $k \geq \mathcal{K}_m$ und $f_1, \ldots, f_k$ eine Menge von irreduziblen Polynomen in $\mathbb{Z}[x]$, sodass für jedes $p \in \mathbb{P}$ ein $n_p \in \mathbb{N}$ mit $p \nmid \prod_{i=1}^k f_i(n_p)$ existiert, es unendlich viele $n \in \mathbb{N}$ gibt, sodass mindestens m der Werte $f_1(n), \ldots, f_k(n)$ prim sind.

Satz 5.1.3. Unter der Annahme von Vermutung 5.1.2 können wir, sofern die Schranken für $\mathcal{K}_m$ dieselben wie für K_m sind, für eine komplexe quadratische Erweiterung $K/\mathbb{Q}$ schließen, dass

1. $\mathcal{S}_{h,K}$ für alle $h \in \mathcal{O}_K$ mit $\Lambda | h$ wahr ist, falls $\mathcal{O}_K$ ein Hauptidealring ist.

2. $\mathcal{S}_{h,K}$ für alle $h \in \mathcal{O}_K$ mit

$$2^{13}3^7 5^4 7^4 11^3 13^3 17^3 19^3 23^3 \prod_{p \in \mathbb{P},\, 29 \leq p \leq 47} p \,|\, h$$

wahr ist, falls $\mathcal{O}_K$ kein Hauptidealring ist.

Beweis. Wir halten uns dicht an den Beweis von Satz 3.1.1. Die Bedingung, dass die benutzen Tupel von irreduziblen Polynomen auch zulässig sind, erhalten wir ähnlich zu Lemma 3.2.2.

1. Dies ergibt sich direkt, da $\mathcal{O}_K$ ein Hauptidealring ist und wir somit dieselben Rechnungen wie für $\mathbb{Z}$ vornehmen können.
2. Wir berechnen für die Menge M_1 aus dem Beweis zu Satz 3.1.1 das kleinste gemeinsame Vielfache der $(b-a)ab$ mit $a, b \in M_1$ und erhalten die Aussage. □

Für den allgemeineren Fall 2 in Satz 4.2.2 wollen wir, dass (2) für unsere primen $\alpha_i r + 1$ gilt und damit

$$2\mathrm{rat}(\alpha_i r) = |\alpha_i r|(c-1) \tag{4}$$

für alle $1 \leq i \leq m$.

5.2 Reelle Erweiterungen

Im Falle $d > 0$ besitzt K eine reelle Einbettung und wir nennen K eine reelle Erweiterung. Die Norm eines Elements muss nicht immer positiv sein, weswegen wir bei der Berechnung von $\phi_K(\alpha r+1)$ und $\phi_K(\beta r+1)$ umsichtiger vorgehen müssen. Eine Möglichkeit, damit wir trotzdem auf die Funktion $D(\alpha, \beta, r)$ zurückgreifen können, ist, dass die Norm von $\alpha r + 1$ und $\beta r + 1$ jeweils positiv ist und $N_K(\alpha)$ und $N_K(\beta)$ dasselbe Vorzeichen besitzen. Wir wählen $\alpha, \beta \in \mathcal{O}_K$, sodass $\mathrm{rat}(\alpha) = \mathrm{rat}(\beta) > 0$, $\beta - \alpha \in \sqrt{d}\mathbb{N}_+$ und $N_K(\alpha), N_K(\beta) > 0$. Wir wollen, dass es unendlich viele $r \in \xi((\alpha-\beta)\alpha\beta)\sqrt{d}\mathbb{Z}$ gibt, sodass $\alpha r + 1$ und $\beta r + 1$ gleichzeitig prim sind. Eine kurze Rechnung zeigt $\alpha r = N_K(\alpha)(\beta - \alpha)\xi(\beta)\sqrt{d}$, dessen Norm und rationaler Anteil positiv sind. Analog folgt dies für βr.

Wir betrachten die Norm von $\alpha r + 1$ erneut. Dabei setzen wir $\alpha = \alpha_1 + \alpha_2\sqrt{d}$, $\beta = \beta_1 + \beta_2\sqrt{d}$ und $r = e\xi((\alpha-\beta)\alpha\beta)\sqrt{d}$ mit $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$. Es ist

$$\begin{aligned} N_K(\alpha r + 1) &= (\alpha r + 1)\xi(\alpha r + 1) \\ &= (eN_K(\alpha)(\beta_2 - \alpha_2)(\beta_1 - \beta_2\sqrt{d})d + 1)(eN_K(\alpha)(\beta_2 - \alpha_2)(\beta_1 + \beta_2\sqrt{d})d + 1) \\ &= e^2 N_K(\alpha)^2(\beta_2 - \alpha_2)^2(\beta_1^2 - \beta_2^2 d)d^2 + 2eN_K(\alpha)(\beta_2 - \alpha_2)\beta_1 d + 1. \end{aligned}$$

Die Diskriminante dieses Polynoms in e ist $\beta_2^2 d$. Da d quadratfrei ist, ist dieses Polynom irreduzibel und wie bei Lemma 3.2.2 sehen wir, dass $N_K(\alpha r+1)$ und $N_K(\beta r+1)$ zusammen ein zulässiges 2-Tupel in der Variablen e bilden.

Vermutung 5.2.1. Seien $\alpha = \alpha_1 + \alpha_2\sqrt{d}$ und $\beta = \beta_1 + \beta_2\sqrt{d}$ mit $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$. Zudem seien $N_K(\alpha), N_K(\beta), \alpha_1 = \beta_1 > 0$. Dann gilt $\mathcal{S}_{h,K}$ für jedes $h \in \mathcal{O}_K$ mit $(\alpha - \beta)\alpha\beta \mid h$.

Diese Vermutung ist wahr, falls Schinzels Vermutung zutrifft.

6 Allgemeine lineare Formen

Ähnlich der Verallgemeinerung der Hardy-Littlewood'schen Vermutung über zulässige k-Tupel zur Dickson'schen Vermutung über zulässigen k-Tupel linearer Formen kann man die Hypothesen $\mathcal{S}_h$ und $\mathcal{T}_h$ für natürliche Zahlen h zu einer Hypothese über lineare Formen aus $\mathbb{Z}[x]$ generalisieren.

6.1 Lösungen zu $\phi(a_1 n + b_1) = \phi(a_2 n + b_2)$

Hierzu seien $l_1 = a_1 x + b_1$ und $l_2 = a_2 x + b_2$ zwei lineare Formen aus $\mathbb{Z}[x]$.

Hypothese $\mathcal{U}_{l_1,l_2}$. Es gilt

$$\phi(a_1 n + b_1) = \phi(a_2 n + b_2)$$

für unendlich viele $n \in \mathbb{N}$.

Wir beginnen mit ein paar einfachen Beobachtungen, die uns ein paar Annahmen über l_1 und l_2 ermöglichen.

1. Wir können die beiden Linearformen so ordnen, dass $a_1 \leq a_2$, da $\mathcal{U}_{l_1,l_2}$ symmetrisch ist.

2. Man kann die ϕ-Funktion in natürlicher Weise mit $\phi(-n) = \phi(n)$ und $\phi(0) = 0$ auf alle ganzen Zahlen erweitern. Da $an + b = -((-a)n + (-b))$, können wir dann auch $a_2 \geq a_1 \geq 0$ annehmen.

3. Sofern $a_1 = 0$ oder $a_2 = 0$, so wissen wir, dass die Gleichung in der Definition von $\mathcal{U}_{l_1,l_2}$ entweder

   (a) immer erfüllt wird, sofern $a_1 = 0, a_2 = 0$ und $\phi(b_1) = \phi(b_2)$.

   (b) nie erfüllt wird, sofern $a_1 = 0, a_2 = 0$ und $\phi(b_1) \neq \phi(b_2)$.

   (c) höchstens endlich oft erfüllt wird, sofern $a_1 = 0$ und $a_2 > 0$, da

   $$\phi(n) > \frac{n}{e^\gamma \log\log n + \frac{3}{\log\log n}}$$

   für alle $n \geq 3$ gilt und die ϕ-Funktion damit keinen Wert unendlich oft annimmt. [7] In der Gleichung sind e die Euler'sche Zahl und γ die Euler'sche Konstante.

   Nur der Fall (a) erfüllt die Hypothese $\mathcal{U}_{l_1,l_2}$.

4. Wir können ohne Beschränkung der Allgemeinheit $a_1 > b_1 \geq 0$ annehmen, weil für $b_1 = ca_1 + d$ mit $a_1 > d \geq 0$ stets

$$\phi(a_1 n + b_1) = \phi(a_2 n + b_2) \Leftrightarrow \phi(a_1(n+c) + d) = \phi(a_2(n+c) + b_2 - ca_2)$$

gilt.

Damit haben wir die linearen Formen in einem gewissen Sinne normalisiert. Der Fall $b_1 = b_2 = 0$ gibt uns erste Ergebnisse.

Lemma 6.1.1. Es gilt $\mathcal{U}_{l_1,l_2}$ für alle l_1, l_2 mit $b_1 = b_2 = 0$ und a_1, a_2 so, dass es ein $g \in \mathbb{N}$ gibt mit $\phi(a_1 g) = \phi(a_2 g)$.

Beweis. Es gilt $\phi(a_1 gn) = \phi(a_1 g)\phi(n) = \phi(a_2 g)\phi(n) = \phi(a_2 gn)$ für alle $n \in \mathbb{N}$ mit $(n, a_1 a_2 g) = 1$. □

Beispiel 6.1.2. Damit gelten zum Beispiel:

1. $\mathcal{U}_{5x,8x}$, da $\phi(8) = \phi(5) = 4$ und damit $\phi(8p) = \phi(5p)$ für jedes $p \in \mathbb{P}_{\geq 7}$.
2. $\mathcal{U}_{16x,17x}$, da für $m = 4$ wir $\phi(16 \cdot 4) = \phi(64) = 32 = 2 \cdot 16 = \phi(4)\phi(17)$ erhalten und so $\phi(16 \cdot 4p) = \phi(17 \cdot 4p)$ für jedes $p \in \mathbb{P}_{\geq 19}$ gilt.

Wir schauen uns Fords Beweise in Unterkapitel 3.2 genauer an, insbesondere

$$m_1 = b'ls(a,b)(a'r+1) \quad \text{und} \quad m_2 = a'ls(a,b)(b'r+1).$$

Die Zahlen a', b' und $s(a,b)$ hängen alle von a und b ab und unsere verschiedenen $r \in \mathbb{N}$ produzieren verschiedene Lösungen $n \in \mathbb{N}$ mit $n = lb'a's(a,b)r$. Jedoch kann $l \in \mathbb{N}_+$ frei gewählt werden, was uns zu unserer nächsten Lösung bringt.

Lemma 6.1.3. Es gilt $\mathcal{U}_{l_1,l_2}$ für alle l_1, l_2 mit $a_1 = a_2 \in \mathbb{N}_+$ beliebig, $b_1 = 0$ und $b_2 = a_1 lh$ für ein beliebiges $l \in \mathbb{N}_+$ und ein $h \in \mathbb{N}$, sodass $h = \kappa(a,b)$ für verschiedene $a < b \in \mathbb{N}$, für die $\mathcal{P}_2(ax+1, bx+1)$ wahr ist.

Beweis. Wir fügen dem Beweis von Lemma 3.2.1 einfach $a_1 \in \mathbb{N}_+$ als Vorfaktor hinzu und erhalten für beliebiges $l \in \mathbb{N}_+$, dass für unendlich viele $r \in \mathbb{N}$ mit $r > \max\{a_1, l, a', b'\}$ sowie $a'r+1$ und $b'r+1$ prim

$$\begin{aligned}\phi(a_1 m_1) &= \phi(a_1 b' ls(a,b))\phi(a'r+1) = \phi(a_1 ls(a,b))b'a'r \\ &= \phi(a_1 a' ls(a,b))\phi(b'r+1) = \phi(a_1 m_2)\end{aligned}$$

und

$$a_1(m_1 - m_2) = a_1(ls(a,b)(b' - a')) = a_1 l\kappa(a,b),$$

was unsere Aussage beweist. $\square$

Beispiel 6.1.4. Indem wir einfach Fords Ergebnisse einsetzen, erhalten wir $\mathcal{U}_{l_1,l_2}$ für

$$\begin{aligned} l_1 &= a_1 x \\ l_2 &= a_1 x + a_1 l \Lambda \end{aligned}$$

mit $a_1, l \in \mathbb{N}$ beliebig beziehungsweise

$$l_2 = a_1 x + 30 a_1 l \quad \text{oder} \quad l_2 = a_1 x + 6 a_1 l,$$

je nachdem, welche Version der Elliott-Halberstam-Vermutung man voraussetzt.

Als nächstes wollen wir uns mit dem Fall $a_1 = 1$ beschäftigen, der wie oben beschrieben sofort $b_1 = 0$ impliziert. Wenn wir uns den Beweis von Lemma 3.2.1 genauer ansehen, so stellen wir fest, dass, sofern alle involvierten Faktoren ungerade sind, auch $\phi(2m_2) = \phi(m_2) = \phi(m_1)$ gilt.

Lemma 6.1.5. Es gibt ein $h \leq 227950$, sodass für alle ungeraden $l \in \mathbb{N}$ die Gleichung

$$\phi(n) = \phi(2n + 2lh)$$

unendlich viele Lösungen $n \in \mathbb{N}$ hat.

Beweis. Wir wählen die Menge

$$\begin{aligned} A = \{&1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, \\ &41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, \\ &77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99\}, \end{aligned}$$

von 50 ungeraden natürlichen Zahlen und betrachten dann erneut die Menge $\mathcal{L} = \{ax+1 : a \in A\}$ von zulässigen Linearformen. Seien wegen Satz 2.2.3 nun $a_1 < a_2$ zwei Elemente aus A, sodass $\mathcal{P}_2(a_1 x + 1, a_2 x + 1)$ wahr ist. Wir wählen $r \in \mathbb{N}$ so, dass $a_1 r + 1$ und $a_2 r + 1$ prim sind und $r > \max\{a_1', a_2', l\}$. Dann gilt für

$$m_1 = a_2' ls(a_1, a_2)(a_1' r + 1), \qquad m_2 = a_1' ls(a_1, a_2)(a_2' r + 1)$$

auch $m_2 - m_1 = l\kappa(a_1, a_2)$ und

$$\phi(2(m_1 + l\kappa(a_1, a_2))) = \phi(2)\phi(m_1 + l\kappa(a_1, a_2)) = \phi(m_1)$$

analog zum Beweis von Lemma 3.2.1. Wir berechnen das Maximum der Menge

$$\{\kappa(a_1, a_2) : a_1, a_2 \in A\}$$

und erhalten 227950. $\square$

6.2 Simultane Lösungen für die ϕ-Funktion im Fall $m \geq 3$

Nun verallgemeinern wir die Hypothese $\mathcal{U}_{l_1,l_2}$ in derselben Art und Weise, in der Ford dies mit $\mathcal{S}_h$ für mehrere simultane Gleichungen tut. Das heißt, wir wollen eine Menge $\mathcal{L} = \{a_1x+b_1, \ldots, a_mx+b_m\}$ von m ganzzahligen Linearformen finden, sodass es unendlich viele $n \in \mathbb{N}$ gibt, die

$$\phi(a_1n + b_1) = \ldots = \phi(a_mn + b_m) \tag{5}$$

erfüllen. Analog zu Lemma 6.1.1 können wir einen Fall abarbeiten.

Lemma 6.2.1. Seien $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathbb{N}$, sodass es ein $g \in \mathbb{N}$ gibt, wofür

$$\phi(a_1g) = \ldots = \phi(a_mg)$$

gilt. Dann gibt es unendlich viele $n \in \mathbb{N}$, die die simultanen Gleichungen

$$\phi(a_1n) = \ldots = \phi(a_mn)$$

erfüllen.

Beweis. Für jedes Paar $1 \leq i < j \leq m$ gilt

$$\phi(a_ign) = \phi(a_ig)\phi(n) = \phi(a_jg)\phi(n) = \phi(a_jgn)$$

für alle $n \in \mathbb{N}$ mit $(n, g\prod_{l=1}^{m} a_l) = 1$. $\square$

Ford [4] zeigte bereits, dass es für jedes $m \in \mathbb{N}_{\geq 2}$ ein $t \in \mathbb{N}$ gibt, sodass es $a_1, \ldots, a_m \in \mathbb{N}$ mit

$$t = \phi(a_1) = \ldots = \phi(a_m)$$

gibt. Damit gibt es für jedes $m \geq 2$ eine Menge von m linearen Formen, die unendlich oft (5) erfüllen.

Lemma 6.2.2. Sei $m \in \mathbb{N}$ und $h_1, \ldots, h_m$ ein m-Tupel natürlicher Zahlen, das wie im Beweis zu Satz 3.1.2 konstruiert wurde. Dann gibt es für jedes $a \in \mathbb{N}$ unendlich viele $n \in \mathbb{N}$, die

$$\phi(a(n + lh_1)) = \ldots = \phi(a(n + lh_m))$$

erfüllen.

Beweis. Wir setzen in den Beweis von 3.1.2 unser beliebiges $a \in \mathbb{N}$ als Vorfaktor ein und sehen direkt, dass für das m-Tupel $\{h_1, \ldots, h_m\}$ auch

$$\phi(a(n + lh_1)) = \ldots = \phi(a(n + lh_m))$$

für jedes $l \in \mathbb{N}$ unendlich oft gilt. □

6.3 Simultane Lösungen für die σ-Funktion

Zuletzt wollen wir ebenso mit der σ-Funktion verfahren. Das bedeutet, wir wollen die Gleichungen

$$\sigma(a_1 n + b_1) = \ldots = \sigma(a_m n + b_m) \tag{6}$$

unendlich oft lösen können. Wir erhalten erneut zwei einfache Fälle.

Lemma 6.3.1. Seien $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathbb{N}$, sodass es ein $g \in \mathbb{N}$ mit

$$\sigma(a_1 g) = \ldots = \sigma(a_m g)$$

gibt. Dann gibt es unendlich viele $n \in \mathbb{N}$, die die simultanen Gleichungen

$$\sigma(a_1 n) = \ldots = \sigma(a_m n)$$

erfüllen.

Beweis. Für jedes Paar $1 \leq i < j \leq m$ gilt

$$\sigma(a_i g n) = \sigma(a_i g)\phi(n) = \sigma(a_j g)\phi(n) = \sigma(a_j g n)$$

für alle $n \in \mathbb{N}$ mit $(n, g\prod_{l=1}^{m} a_l) = 1$. □

Adams-Watters [3] zeigt, dass aus einer stärkeren Version der Goldbach-Vermutung gezeigt werden kann, dass 5 die einzige ungerade Zahl $t \in \mathbb{N}$ ist, sodass es kein $n \in \mathbb{N}$ mit $s(n) = \sigma(n) - n = t$ gibt. Man nennt solch eine Zahl *unberührbar*. Von Hardy und Littlewood vermutet und von Landau bewiesen [2] wurde, dass die Anzahl der Goldbach-

Repräsentationen, d. h. die Anzahl der verschiedenen Paare $p \neq q \in \mathbb{P}_{\geq 3}$, sodass $n = p+q$, asymptotisch steigt. Für

$$n = p_1 + q_1 = p_2 + q_2$$

sind die Summen der echten Teiler von p_1q_1 und p_2q_2, nämlich

$$s(p_1q_1) = p_1 + q_1 + 1 = p_2 + q_2 + 1 = s(p_2q_2) = n + 1,$$

gleich. Ob es eine ähnliche Aussage für die σ-Funktion gibt, ist offen. Unter der Annahme, dass dies zutrifft und es für jedes $m \in \mathbb{N}$ ein $t \in \mathbb{N}$ gibt, sodass es $a_1, \ldots, a_m \in \mathbb{N}$ mit $\sigma(a_1) = \ldots = \sigma(a_m)$ gibt, können wir für jedes m auch solch ein m-Tupel an passenden linearen Formen finden.

Lemma 6.3.2. Sei $m \in \mathbb{N}$ und $h_1, \ldots, h_m$ ein m-Tupel natürlicher Zahlen, das wie im Beweis zu Satz 3.1.4 konstruiert wurde. Dann gibt es für jedes $a \in \mathbb{N}$ unendlich viele $n \in \mathbb{N}$, die

$$\sigma(a(n + lh_1)) = \ldots = \sigma(a(n + lh_m))$$

erfüllen.

Beweis. Analog zu 6.2.2 sehen wir, dass die Zunahme eines Vorfaktors den Beweis zu Satz 3.1.4 nicht ungültig macht. $\square$

Literatur

[1] A. Castillo, C. Hall, R. J. Lemke Oliver, P. Pollack und L. Thompson, *Bounded gaps between primes in number fields*, Proceedings of the American Mathematical Society, 143 (2015), pp. 2841–2856.

[2] D. A. Goldston und L. Yang, *The average number of Goldbach representations*, in Prime Number and Representation Theory, vol. 2, Lecture Series of Modern Number Theory, 2017, pp. 1 – 12.

[3] F. Adams-Watters und E. W. Weisstein, *Untouchable number.* MathWorld–A Wolfram Web Resource. `https://mathworld.wolfram.com/UntouchableNumber.html`, 2006.

[4] K. Ford, *The number of solutions of $\phi(x) = m$*, Ann. of Math., 150 (1999), pp. 283–311.

[5] ——, *Solutions of $\phi(n) = \phi(n + k)$ and $\sigma(n) = \sigma(n + k)$.* `https://arxiv.org/abs/2002.12155v5`, 2020.

[6] G. H. Hardy, E. M. Wright, D. R. Heath-Brown und J. H. Silverman, *An Introduction to the Theory of Numbers, Sixth Edition*, Oxford University Press, 2008.

[7] J. B. Rosser und L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics, 6 (1962).

[8] H. Koch, *Algebraic Number Theory*, Springer, 1997.

[9] J. Maynard, *Small gaps between primes*, Ann. of Math., 181 (2015), pp. 383 – 413.

[10] ——, *Dense clusters of primes in subsets*, Compos. Math., 152 (2016), pp. 1517 – 1554.

[11] M. Orr, *Algebraic Number Theory*, Vorlesungsmitschrift, 2019.

[12] D. Polymath, *Variants of the Selberg sieve and bounded intervals containing many primes*, Res. Math. Sci., 1 (2014). Art. 12.

[13] S. W. Graham, J. J. Holt und C. Pomerance, *On the solutions $\phi(n) = \phi(n + k)$*, in Number Theory in Progress, vol. 2 (1999), de Gruyter, 1997, pp. 867 – 882.

[14] Z. Parker, J. Rushall und J. Hunt, *Perfect numbers in the ring of Eisenstein integers.* `https://arxiv.org/abs/1602.09106v1`, 2016.