ETH Zürich

Bachelorarbeit

Selbergs elementarer Beweis des Dirichletschen Primzahlsatzes

Autorin:
Salome Schumacher

Betreuer:
Prof. Richard Pink

1. Oktober 2014

Inhaltsverzeichnis

1 Einleitung

Ziel dieser Bachelorarbeit ist es, den folgenden Satz zu beweisen:

Satz 1.1 (Dirichletscher Primzahlsatz) *Seien k und l positive, teilerfremde ganze Zahlen. Dann gibt es unendlich viele Primzahlen, die kongruent zu l modulo k sind.*

Es ist klar, dass für nicht relativ prime k und l der Satz in der obigen Form nicht wahr ist. Denn ist $d := (l, k) \neq 1$, so erhalten wir mit $k' := \frac{k}{d} \in \mathbb{Z}$ und $l' := \frac{l}{d} \in \mathbb{Z}$ für jedes $n \in \mathbb{Z}_{\geq 1}$

$$kn + l = d(k'n + l').$$

Daher ist $kn + l$ nicht prim.

Im Jahre 1808 veröffentlichte Adrien-Marie Legendre einen vermeintlichen Beweis des Dirichletschen Primzahlsatzes. Leider hatte sich – versteckt hinter den Worten „Es ist leicht zu sehen, dass ...“– ein Fehler eingeschlichen. 1837 gelang Peter Gustav Lejeune Dirichlet der erste korrekte Beweis des Satzes. Über hundert Jahre später publizierte Atle Selberg 1949 einen elementaren Beweis des Dirichletschen Primzahlsatzes, dem wir in dieser Arbeit folgen werden. Genauer werden wir folgende Aussage beweisen:

Satz 1.2 *Für jede positive ganze Zahl k gibt es positive reelle Zahlen C_k und x_0, die nur von k abhängen, so dass für jede positive ganze Zahl l mit $(k, l) = 1$*

$$\sum_{\substack{p \leq x \\ p \equiv l(k)}} \frac{\log p}{p} > C_k \log x$$

für alle $x > x_0$ gilt. Dabei läuft die Summe über alle Primzahlen $p \leq x$, die die Bedingung $p \equiv l(k)$ erfüllen.

Aus diesem Satz folgt der Dirichletsche Primzahlsatz, denn gäbe es nur endlich viele Primzahlen, die kongruent zu l modulo k sind, so wäre die linke Seite beschränkt, die rechte strebt aber gegen unendlich, wenn x gegen unendlich strebt.

2 Arithmetische Funktionen

2.1 Definitionen und partielle Summation

Bemerkung 2.1 *Sofern nichts anderes gesagt wird, seien im Folgenden p,q und r Primzahlen, n,m,k und l positive ganze Zahlen und k und l teilerfremd.*

Definition 2.2 *Die Möbiusfunktion $\mu : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ ist wie folgt definiert:*

$$\mu(1) = 1;$$

Für $x > 1$ sei $x = p_1^{a_1} \dots p_k^{a_k}$ die kanonische Primfaktorzerlegung von x. Dann ist

$$\mu(x) = \begin{cases} (-1)^k, & \text{wenn } a_1 = a_2 = \dots = a_k = 1 \\ 0 & \text{sonst.} \end{cases}$$

Definition 2.3 *Die eulersche Phi-Funktion $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ gibt für jedes $x \in \mathbb{Z}_{\geq 1}$ an, wie viele zu x teilerfremde positive ganze Zahlen es gibt, die x nicht übersteigen. Das heisst:*

$$\varphi(x) = \sum_{\substack{1 \leq k \leq x \\ (k,x)=1}} 1.$$

Definition 2.4 *Die Mangoldt-Funktion $\Lambda : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ ist wie folgt definiert:*

$$\Lambda(x) = \begin{cases} \log p, & \text{wenn } x = p^m \text{ für eine Primzahl } p \text{ und ein } m \in \mathbb{Z}_{\geq 1}, \\ 0 & \text{sonst.} \end{cases}$$

Definition 2.5 *Die Primzahlfunktion $\pi : \mathbb{R} \to \mathbb{R}$ ist definiert als die Anzahl Primzahlen, die x nicht übersteigen:*

$$\pi(x) = \sum_{p \leq x} 1.$$

Definition 2.6 *Die Tschebyschow-Funktionen $\vartheta : \mathbb{R}_{>0} \to \mathbb{R}$ und $\psi : \mathbb{R}_{>0} \to \mathbb{R}$ sind wie folgt definiert:*

$$\psi(x) = \sum_{n \leq x} \Lambda(n)$$

und

$$\vartheta(x) = \sum_{p \leq x} \log p.$$

Satz 2.7 *(Abelsche partielle Summation) Für jede Funktion $a : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ und jedes $x \in \mathbb{R}$ sei*

$$A(x) := \sum_{n \leq x} a(n),$$

wobei $A(x) := 0$, ist für alle $x < 1$. Angenommen $f \in C^1([y, x])$, für ein $y \in \mathbb{R}$ mit $0 < y < x$. Dann gilt:

$$\sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Beweis. Sei $k := \lfloor x \rfloor$ und $m := \lfloor y \rfloor$. Dann ist $A(x) = A(k)$ und $A(y) = A(m)$. Also:

$$\begin{aligned}\sum_{y < n \leq x} a(n)f(n) = \sum_{n=m+1}^{k} a(n)f(n) &= \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}f(n) \\ &= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\ &= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1)\end{aligned}$$

An dieser Stelle können wir den Hauptsatz der Differential- und Integralrechnung anwenden und somit ist der letzte Ausdruck gleich

$$\begin{aligned}&- \sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1) \\ &\qquad = - \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1).\end{aligned}$$

Hier verwenden wir erneut den Hauptsatz und erhalten

$$\begin{aligned}\sum_{y < n \leq x} a(n)f(n) = &- \int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_k^x A(t)f'(t)dt - A(y)f(y) \\ &- \int_y^{m+1} A(t)f'(t)dt \\ &= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt. \qquad \square\end{aligned}$$

2.2 Der schwache Primzahlsatz

Der Primzahlsatz besagt, dass

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

ist. Diesen Satz zu beweisen würde den Rahmen dieser Arbeit sprengen. Zwei unterschiedliche Beweise findet man jedoch in [1, S.278-291] und in [8]. Glücklicherweise ist für viele Zwecke – so auch für unsere – die folgende schwächere Form des Primzahlsatzes ausreichend:

Satz 2.8 *Für alle $x \in \mathbb{R}_{\geq 2}$ gilt*

$$\frac{1}{6}\frac{x}{\log x} < \pi(x) \leq \frac{4x}{\log x}.$$

Insbesondere ist

$$\pi(x) = O\left(\frac{x}{\log x}\right).$$

Dieser Satz lässt sich deutlich einfacher beweisen als der Primzahlsatz. Wir werden jedoch nur die Abschätzung nach oben zeigen, da die andere Abschätzung für den Beweis von Satz 1.2 nicht benötigt wird.

Lemma 2.9 *Für alle ganzen Zahlen $x \geq 1$ gilt $\vartheta(x) \leq 2x \log 2$. Insbesondere ist $\vartheta(x) = O(x)$.*

Beweis. Sei $m \in \mathbb{Z}_{\geq 1}$ und

$$M := \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m}.$$

M ist ganzzahlig, da M ein Binomialkoeffizient ist. Der binomische Lehrsatz besagt insbesondere, dass

$$(1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k}$$

ist. Da $M = \binom{2m+1}{m} = \binom{2m+1}{m+1}$ ist, kommt M in obiger Summe zwei Mal vor. Daher erhalten wir:

$$2^{2m+1} \geq 2M \Rightarrow 2^{2m} \geq M.$$

Für $m+1 < p \leq 2m+1$ gilt $p \mid (2m+1)!$ aber auch $p \nmid m!(m+1)!$. Daher folgt

$$\left(\prod_{m+1<p\leq 2m+1} p\right) \mid M$$

und auch

$$\sum_{m+1<p\leq 2m+1} \log p \leq \log M \leq \log 2^{2m} = 2m \log 2. \tag{1}$$

Nun können wir das Lemma per Induktion beweisen. Die Fälle $x = 1$ und $x = 2$ sind klar. Angenommen $\vartheta(x) \leq 2x \log 2$ für alle $x \leq x_0 - 1$, wobei $x_0 \in \mathbb{Z}_{\geq 3}$ ist. Sei x_0 zunächst gerade. Dann gilt:

$$\vartheta(x_0) = \vartheta(x_0 - 1) \leq 2(x_0 - 1)\log 2 \leq 2x_0 \log 2.$$

Sei nun x_0 ungerade. Das heisst $x_0 = 2n + 1$ für ein $n \in \mathbb{Z}_{\geq 1}$. Dann gilt:

$$\begin{aligned}\vartheta(x_0) = \vartheta(2n+1) &= (\vartheta(2n+1) - \vartheta(n+1)) + \vartheta(n+1) \\ &\leq 2n\log 2 + 2(n+1)\log 2 = 2(2n+1)\log 2 = 2x_0 \log 2,\end{aligned}$$

wobei bei der Ungleichung die Induktionsvoraussetzung und (1) verwendet wurden. □

Beweis (von Satz 2.8). Sei $0 < \alpha < 1$. Dann folgt mit Lemma 2.9:

$$(\pi(x) - \pi(x^\alpha)) \log x^\alpha = \sum_{p \le x} \log x^\alpha - \sum_{p \le x^\alpha} \log x^\alpha$$
$$= \sum_{x^\alpha < p \le x} \log x^\alpha \le \sum_{x^\alpha < p \le x} \log p \le \vartheta(x) \le 2x \log 2.$$

Also gilt:

$$\pi(x) \le \frac{2x \log 2}{\log x^\alpha} + \pi(x^\alpha) \le \frac{2x \log 2}{\alpha \log x} + x^\alpha = \frac{x}{\log x}\left(\frac{2 \log 2}{\alpha} + \frac{\log x}{x^{1-\alpha}}\right)$$

Die Funktion $\frac{\log x}{x^{1-\alpha}}$ nimmt ihr Maximum bei $e^{\frac{1}{1-\alpha}}$ an. Somit ist

$$\pi(x) \le \frac{x}{\log x}\left(\frac{2 \log 2}{\alpha} + \frac{1}{(1-\alpha)e}\right).$$

Wenn wir nun $\alpha = \frac{2}{3}$ eingesetzen, erhalten wir $\pi(x) \le \frac{4x}{\log x}$. □

2.3 Eine Abschätzung von $\sum_{p \le x} \frac{\log^n p}{p}$

Lemma 2.10 *Für alle $x \in \mathbb{R}_{\ge 1}$ gilt:*

$$\sum_{n \le x} \log n = \sum_{n \le x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor.$$

Beweis. Sei $x \in \mathbb{R}_{\ge 1}$. Dann hat $\lfloor x \rfloor! = 1 \cdot 2 \cdots \lfloor x \rfloor$ genau $\left\lfloor \frac{\lfloor x \rfloor}{p} \right\rfloor = \left\lfloor \frac{x}{p} \right\rfloor$ Faktoren, die durch p teilbar sind. Dies sind $p, 2p, 3p, \ldots$. Von diesen sind genau $\left\lfloor \frac{\lfloor x \rfloor}{p^2} \right\rfloor = \left\lfloor \frac{x}{p^2} \right\rfloor$ Faktoren auch durch p^2 teilbar. Wenn wir diese Überlegung fortführen, erkennen wir, dass $\lfloor x \rfloor!$ den Primfaktor p genau

$$\sum_{k=1}^{\infty} \left\lfloor \frac{x}{p^k} \right\rfloor$$

mal enthält. Das heisst

$$\sum_{n \le x} \log n = \log \lfloor x \rfloor! = \sum_{p \le x} \log p \sum_{k=1}^{\infty} \left\lfloor \frac{x}{p^k} \right\rfloor = \sum_{n \le x} \left\lfloor \frac{x}{n} \right\rfloor \Lambda(n).$$

Alternativ kann dieses Lemma auch mit [1, Satz 3.11] und [1, Satz 2.10] hergeleitet werden. □

Satz 2.11 *Für alle $x \in \mathbb{R}_{\ge 1}$ gilt:*

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1).$$

Beweis. ***Behauptung 1*** : $\psi(x) = O(x)$
Mit $\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{p^m \le x} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \le x^{\frac{1}{m}}} \log p$ folgt

$$0 \le \psi(x) - \vartheta(x) = \sum_{m=2}^{\infty} \sum_{p \le x^{\frac{1}{m}}} \log p = \sum_{m=2}^{\log_2 x} \sum_{p \le x^{\frac{1}{m}}} \log p$$
$$\le \sum_{m=2}^{\log_2 x} x^{\frac{1}{m}} \log x^{\frac{1}{m}} \le \frac{\log x}{\log 2} \sqrt{x} \log \sqrt{x} = \frac{\sqrt{x} \log^2 x}{2 \log 2}.$$

Also folgt mit Lemma 2.9 $\psi(x) = O(x)$.

Behauptung 2 : $\sum_{n\leq x}\frac{\Lambda(n)}{n}=\log x+O(1)$
Mit Satz 2.7 erhalten wir mit der Wahl $a(n):=1$ und $f(t):=\log t$:

$$\sum_{n\leq x}\log n=x\log x+O\Big(\int_1^x t\frac{1}{t}dt\Big)=x\log x+O(x).$$

Also folgt mit Lemma 2.10:

$$x\log x+O(x)=\sum_{n\leq x}\log n=\sum_{n\leq x}\Lambda(n)\lfloor\frac{x}{n}\rfloor=x\sum_{n\leq x}\frac{\Lambda(n)}{n}+O(\psi(x))$$

Mit Behauptung 1 erhalten wir:

$$x\log x=x\sum_{n\leq x}\frac{\Lambda(n)}{n}+O(x).$$

Daher folgt Behauptung 2.

Mit obigen zwei Behauptungen können wir nun den Satz beweisen:

$$0\leq\sum_{n\leq x}\frac{\Lambda(n)}{n}-\sum_{p\leq x}\frac{\log p}{p}=\sum_{m=2}^{\infty}\sum_{p^m\leq x}\frac{\log p}{p^m}\leq\sum_p\sum_{k=2}^{\infty}\frac{1}{p^k}\log p$$
$$=\sum_p\frac{\log p}{p(p-1)}\leq\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}<\infty$$

Mit Behauptung 2 folgt der Satz. □

Korollar 2.12 *Für alle $x\in\mathbb{R}$ und alle $m\in\mathbb{Z}_{\geq 1}$ gilt:*

$$\sum_{p\leq x}\frac{\log^m p}{p}=\frac{\log^m x}{n}+O(\log^{m-1}x)$$

Beweis. Der Fall $m=1$ folgt aus Satz 2.11. Betrachten wir nun den Fall $m>1$. Wir benutzen Satz 2.7 mit

$$a(n):=\begin{cases}\frac{\log n}{n}, & \text{wenn } n \text{ prim}\\ 0 & \text{sonst}\end{cases}\qquad\text{und}\qquad f(t):=\log^{m-1}t,$$

wobei $n\in\mathbb{Z}_{\geq 2}$ und $t\in\mathbb{R}_{\geq 2}$ ist. Ausserdem verwenden wir Satz 2.11. Somit erhalten wir:

$$\sum_{p\leq x}\frac{\log^m p}{p}=\Big(\sum_{p\leq x}\frac{\log p}{p}\Big)\log^{m-1}x-(m-1)\int_2^x\Big(\sum_{p\leq t}\frac{\log p}{p}\Big)\frac{\log^{m-2}t}{t}dt+O(1)$$
$$=\{\log x+O(1)\}\log^{m-1}x-(m-1)\int_2^x\{\log t+O(1)\}\frac{\log^{m-2}t}{t}dt=\frac{\log^m x}{n}+O(\log^{m-1}x).$$ □

3 Charaktere und Kongruenzen

Definition 3.1 *Sei G eine endliche abelsche Gruppe der Ordnung h mit den Elementen $\{a_1,a_2,\ldots,a_h\}$. Ein abelscher Charakter von G ist eine Funktion $\chi:G\to\mathbb{C}$, so dass für alle $i,j\in\{1,2,\ldots,h\}$*

$$\chi(a_i)\chi(a_j)=\chi(a_ia_j)$$

ist und es ein $i\in\{1,2,\ldots,h\}$ gibt mit

$$\chi(a_i)\neq 0.$$

Ist $G=\big(\frac{\mathbb{Z}}{m\mathbb{Z}}\big)^{\times}$ für ein $m\in\mathbb{Z}_{\geq 1}$, so nennt man χ einen Dirichlet-Charakter.

Bemerkung 3.2 *Seien $s \in \mathbb{Z}$ und $k \in \mathbb{Z}_{\geq 1}$. Im Folgenden werden wir mit $\hat{s}$ die zu s gehörende Restklasse modulo k bezeichnen. Wir nennen s einen Repräsentanten der Restklasse $\hat{s}$.*

Bemerkung 3.3 *Sei $G = \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$ für ein $m \in \mathbb{Z}_{\geq 1}$. Zu einem Dirichlet-Charakter $\psi : G \to \mathbb{C}$ wie oben definiert, kann man eine Funktion $\chi : \mathbb{Z} \to \mathbb{C}$ wie folgt definieren:*

$$\chi(k) = \begin{cases} \psi(\hat{k}), & \text{wenn } (k,m) = 1 \\ 0 & \text{sonst.} \end{cases}$$

Auch diese Funktion wird Dirichlet-Charakter genannt.

Bemerkung 3.4 *Für jedes $m \in \mathbb{Z}_{\geq 1}$ gibt es genau $\varphi(m)$ viele Dirichlet-Charaktere modulo m. Einen Beweis dazu findet man beispielsweise in [1, Satz 6.8].*

Bemerkung 3.5 *Für jedes $m \in \mathbb{Z}_{\geq 1}$ ist $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$ eine Gruppe mit $\varphi(m)$ Elementen. Aus den Gruppeneigenschaften folgen insbesondere die Lemmata 3.6 und 3.7.*

Lemma 3.6 *Sei $A = \{a_1, a_2, \ldots, a_n\}$ eine Menge paarweise verschiedener primer Restklassen modulo k und sei $(k,t) = 1$ für ein $t \in \mathbb{Z}$. Dann ist $\{\hat{t}a_1, \hat{t}a_2, \ldots, \hat{t}a_n\}$ ebenfalls eine Menge paarweise verschiedener primer Restklassen modulo k.*

Lemma 3.7 *Seien a und m teilerfremde ganze Zahlen. Dann hat die lineare Kongruenz*

$$ax \equiv b(m)$$

genau eine Lösung modulo m.

Definition 3.8 *Eine Menge bestehend aus m Repräsentanten, einer aus jeder Restklasse modulo m, wird vollständiges Restklassensystem modulo m genannt.*

Lemma 3.9 *Seien h und k positive ganze Zahlen und $M = \{m_1, m_2, \ldots, m_h\}$ eine Menge von Repräsentanten, die zu k teilerfremd sind, aus paarweise verschiedenen Restklassen modulo k. Ausserdem sei l eine positive ganze Zahl, die zu k teilerfremd ist. Weiter nehmen wir an, dass $h \geq \frac{1}{2}\varphi(k)$ ist und dass zu jedem reellen Dirichlet-Charakter χ modulo k ein $m \in M$ existiert mit $\chi(\hat{m}) = 1$. Ausserdem soll es $m, m' \in M$ geben mit $mm' \equiv l(k)$. Dann gibt es $m, m', m'' \in M$ mit*

$$mm'm'' \equiv l(k).$$

Beweis. Wir beweisen dieses Lemma indirekt. Angenommen

$$m_{i_1} m_{i_2} m_{i_3} \not\equiv l(k)$$

für alle $i_1, i_2, i_3 \in \{1, 2, \ldots, h\}$. Dies ist äquivalent zur Aussage, dass

$$m_{i_1} m_{i_2} \not\equiv l\bar{m_{i_3}}(k) \tag{2}$$

ist für alle $i_1, i_2, i_3 \in \{1, 2, \ldots, h\}$. Dabei haben wir $\bar{m_{i_3}}$ so definiert, dass $m_{i_3}\bar{m_{i_3}} \equiv 1(k)$ ist. Sei zunächst $h > \frac{1}{2}\varphi(k)$. In diesem Fall sind nach Lemma 3.6

$$\hat{m_1}\hat{m_1}, \hat{m_1}\hat{m_2}, \ldots, \hat{m_1}\hat{m_h}$$

paarweise verschiedene Elemente aus $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$. Das heisst also

$$m_1 m_1, m_1 m_2, \ldots, m_1 m_h$$

sind paarweise verschieden modulo k und daher nimmt die linke Seite von (2) mehr als $\frac{1}{2}\varphi(k)$ Werte modulo k an. Ebenso nimmt die rechte Seite von (2) mehr als $\frac{1}{2}\varphi(k)$ verschiedene Werte modulo k an. Da $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$ Ordnung $\varphi(k)$ hat, muss es im Widerspruch zur Annahme $i_1, i_2, i_3 \in \{1, \ldots, h\}$ geben mit $m_{i_1} m_{i_2} \equiv l\bar{m_{i_3}}(k)$.
Sei nun $h = \frac{1}{2}\varphi(k)$. Damit wir keinen Widerspruch zu (2) erhalten, kann das Produkt $m_{i_1} m_{i_2}$

nur genau h verschiedene Werte modulo k annehmen. Wir definieren $n_i := m_i\bar{m}_1$. Die h Restklassen

$$\hat{n_1} = \hat{1}, \hat{n_2}, \hat{n_3}, \ldots, \hat{n_h}$$

sind gemäss Lemma 3.6 paarweise verschieden.

Behauptung 1: Die Menge $N := \{\hat{n_1}, \hat{n_2}, \ldots, \hat{n_h}\}$ bildet zusammen mit der Restklassenmultiplikation eine Untergruppe von $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$.

Beweis. Wir definieren $G := \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$. Seien $i, j \in \{1, 2, \ldots, h\}$. Weil das Produkt $m_i m_j$ genau h verschiedene Werte annehmen kann, gibt es auch, weil

$$\hat{n_i}\hat{n_j} = \hat{m_i}\hat{m_j}\hat{\bar{m}_1}\hat{\bar{m}_1}$$

ist, genau h verschiedene Produkte $\hat{n_i}\hat{n_j}$. Da aber die Menge

$$\{\hat{n_1}\hat{n_1}, \hat{n_1}\hat{n_2}, \ldots, \hat{n_1}\hat{n_j}\} = N$$

bereits h verschiedene Elemente besitzt, folgt, dass $\hat{n_i}\hat{n_j} \in N$ ist. Das heisst, N ist abgeschlossen bezüglich der Restklassenmultiplikation.
Sei nun $j \in \{1, 2, \ldots, h\}$. Mit Lemma 3.6 erhalten wir, dass die Menge

$$\{\hat{n_1}\hat{n_j}, \hat{n_2}\hat{n_j}, \ldots, \hat{n_h}\hat{n_j}\}$$

aus genau h paarweise verschiedenen Elementen besteht. Daraus folgt:

$$\{\hat{n_1}\hat{n_j}, \hat{n_2}\hat{n_j}, \ldots \hat{n_h}\hat{n_j}\} = N.$$

Weil $\hat{1} \in N$ ist, gibt es ein $i \in \{1, 2, \ldots, h\}$ mit $\hat{n_i}\hat{n_j} = \hat{1}$. Also besitzt $\hat{n_j}$ ein Inverses in N. □

Nun können wir auf $G = \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$ wie folgt eine Funktion $\chi : G \to \mathbb{C}$ definieren:

$$\chi(\hat{n}) = \begin{cases} 1, & \text{wenn } \hat{n} \in N \\ -1, & \text{wenn } \hat{n} \in G \setminus N \end{cases}$$

Behauptung 2: χ ist ein reeller Dirichlet-Charakter.

Beweis. Wir müssen zeigen, dass für alle $a, b \in G$ $\chi(a)\chi(b) = \chi(ab)$ gilt. Betrachten wir die Faktorgruppe $\frac{G}{N}$. Diese hat Ordnung 2. Also folgt, dass $\frac{G}{N} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$ ist. Seien nun $a, b \notin N$. Da in $\frac{\mathbb{Z}}{2\mathbb{Z}}$ 1+1=0 ist folgt, dass $ab \in N$ ist und daher auch

$$\chi(ab) = 1 = \chi(a)\chi(b).$$

Analog folgt, dass für $a \in N$ und $b \notin N$ auch $ab \notin N$ ist und für $a, b \in N$ auch $ab \in N$ ist. □

Für den Dirichlet-Charakter χ gilt weiter

$$\chi(\hat{m_i}) = \chi(\hat{n_i}\hat{m_1}) = \chi(\hat{n_i})\chi(\hat{m_1}) = \chi(\hat{m_1})$$

für alle $i \in \{1, 2, \ldots, h\}$. Da es nach Voraussetzung mindestens ein $m_i \in M$ gibt mit $\chi(\hat{m_i}) = 1$, gilt $\chi(\hat{m_i}) = 1$ für alle $i \in \{1, 2, \ldots, h\}$. Also

$$\chi(\hat{l}) = \chi(\hat{m}\hat{m'}) = \chi(\hat{m})\chi(\hat{m'}) = 1.$$

Folglich sind $1, l \in M$. Da

$$1 \cdot 1 \cdot l \equiv l(k)$$

ist, haben wir einen Widerspruch zu (2). Damit ist Lemma 3.9 bewiesen. □

Definition 3.10 *Seien a und c teilerfremde ganze Zahlen. Dann nennt man a einen quadratischen Rest modulo c, wenn die Kongruenz $x^2 \equiv a(c)$ eine Lösung in $\mathbb{Z}$ hat. Wenn die Kongruenz keine Lösung hat, so nennt man a einen quadratischen Nichtrest modulo c.*

Definition 3.11 *Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$. Das Legendre-Symbol ist wie folgt definiert:*

$$\left(\frac{a}{p}\right)_L = \begin{cases} 1, & \text{wenn } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{wenn } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

Definition 3.12 *Seien $P \in \mathbb{Z}_{\geq 1}$ ungerade und $a \in \mathbb{Z}$ mit $(a, P) = 1$. Dann definieren wir das Jacobi-Symbol wie folgt:*

$$\left(\frac{a}{P}\right)_J = \begin{cases} 1, & \text{wenn } P = 1 \text{ ist,} \\ \left(\frac{a}{p_1}\right)_L^{m_1} \left(\frac{a}{p_2}\right)_L^{m_2} \dots \left(\frac{a}{p_k}\right)_L^{m_k}, & \text{wenn } P = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}. \end{cases}$$

Wenn $(a, P) > 1$ ist, so sei $\left(\frac{a}{P}\right)_J = 0$.

Definition 3.13 *Seien $c \in \mathbb{Z}_{\geq 1}$ und $a \in \mathbb{Z} \setminus \{0\}$. Wenn $c \neq 0$ ist, so definieren wir das Kronecker-Symbol mit Hilfe des Jacobi-Symbols wie folgt:*

$$\left(\frac{a}{c}\right) = \left(\frac{2^\nu}{a}\right)_J \left(\frac{a}{b}\right)_J,$$

wobei $c = 2^\nu b$ ist mit einer ungeraden ganzen Zahl b und einem $\nu \in \mathbb{Z}_{\geq 0}$. Für $c = 0$ definieren wir das Kronecker-Symbol wie folgt:

$$\left(\frac{a}{0}\right) = \begin{cases} 1, & \text{wenn } a = 1 \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

Definition 3.14 *Die kleinste positive ganze Zahl f für die*

$$a^f \equiv 1(m)$$

ist, heisst Exponent von a modulo m. Wir schreiben

$$f = \exp_m(a).$$

Wenn $\exp_m(a) = \varphi(m)$ ist, so ist a eine Primitivwurzel modulo m.

Satz 3.15 *Sei $m \in \mathbb{Z}_{\geq 1}$. Für jeden reellen, nicht trivialen Dirichlet-Charakter χ modulo m gibt es eine ganze Zahl D, die kein Quadrat ist mit*

$$\chi(n) = \left(\frac{D}{n}\right),$$

wenn $n > 0$ ist. Ausserdem kann ein solches D gefunden werden, das $|D| \leq m^2$ erfüllt.

Beweis. Die Sätze und Herleitungen, auf die in diesem Beweis verwiesen wird, werden ausführlich in [1] besprochen.

1.Fall: Sei $\alpha \in \mathbb{Z}_{\geq 1}$. Des Weiteren seien p eine ungerade Primzahl und χ ein reeller Dirichlet-Charakter modulo p^α.
Sei $n \in \mathbb{Z}_{\geq 1}$ teilerfremd zu p. Nach [1, S.218] sind alle Dirichlet-Charaktere modulo p^α gegeben durch

$$\chi_h(n) = \exp\left(\frac{2\pi i h b(n)}{\varphi(p^\alpha)}\right) \qquad h \in \{0, 1, \dots, \varphi(p^\alpha) - 1\}.$$

Dabei ist $b(n)$ wie folgt definiert: Sei g eine Primitivwurzel modulo p. Dann ist $b(n)$ die eindeutige ganze Zahl, die

$$n \equiv g^{b(n)}(p^\alpha) \qquad \text{und} \qquad 0 \leq b(n) < \varphi(p^\alpha)$$

erfüllt. Nach [1, Satz 10.12] ist χ_h genau dann reell, wenn $h = 0$ oder $h = \frac{\varphi(p^\alpha)}{2}$ ist. χ_0 ist der triviale Dirichlet-Charakter modulo p^α. Somit ist er einzige nicht triviale, reelle Dirichlet-Charakter modulo p^α gegeben durch

$$\chi_{\frac{\varphi(p^\alpha)}{2}}(n) = \exp(\pi i b(n)) = (-1)^{b(n)}.$$

Nach [1, Satz 10.5] ist $b(n)$ genau dann gerade, wenn die Kongruenz

$$n \equiv x^2(p^\alpha)$$

eine Lösung hat. Daher erhalten wir

$$\chi_{\frac{\varphi(p^\alpha)}{2}}(n) = (-1)^{b(n)} = \left(\frac{n}{p}\right).$$

Mit dem quadratischen Reziprozitätssatz für das Kronecker-Symbol erhalten wir also

$$\left(\frac{n}{p}\right) = \left(\frac{p^*}{n}\right),$$

wobei $p^* = p$ ist, wenn $p \equiv 1(4)$ und $p^* = -p$ ist, wenn $p \equiv -1(4)$. Zusammengefasst erhalten wir:

$$\chi(n) = \left(\frac{p^*}{n}\right).$$

Das heisst, die einzigen reellen Dirichlet-Charaktere modulo p^α sind gegeben durch:

$$\chi_0(n) = \chi_{\varphi(p^\alpha)}(n) = (\chi_{\frac{\varphi(p^\alpha)}{2}}(n))^2 = \left(\frac{p^2}{n}\right)$$

und

$$\chi_{\frac{\varphi(p^\alpha)}{2}}(n) = \left(\frac{p^*}{n}\right).$$

2.Fall: Sei χ ein reeller Dirichlet-Charakter modulo 2^α für ein $\alpha \in \mathbb{Z}_{\geq 1}$.
Sei $n \in \mathbb{Z}_{\geq 1}$ mit $(n, 2) = 1$. Betrachten wir zuerst den Fall $\alpha \geq 3$. Wir definieren:

$$f(n) := (-1)^{\frac{n-1}{2}} \qquad\qquad g(n) := \exp\left(\frac{2\pi i b(n)}{h}\right),$$

wobei $h := \frac{\varphi(2^\alpha)}{2}$ ist und $b(n)$ die eindeutige ganze Zahl ist, die Bedingungen

$$n \equiv (-1)^{\frac{n-1}{2}} 5^{b(n)}(2^\alpha) \qquad\qquad 1 \leq b(n) \leq \frac{\varphi(2^\alpha)}{2}$$

erfüllt. Nach [1, S.219] haben alle Dirichlet-Charaktere modulo 2^α die Form (siehe [1, Satz 10.11])

$$\chi_{a,c}(n) = f(n)^a g(n)^c,$$

wobei $a \in \{1, 2\}$ und $c \in \{1, 2, \ldots, \frac{\varphi(2^\alpha)}{2}\}$ ist. Nach [1, Satz 10.13] ist $\chi_{a,c}$ genau dann reell, wenn $c = h$ oder $c = \frac{h}{2}$ ist. Das heisst, es gibt genau vier reelle Dirichlet-Charaktere modulo 2^α. Betrachten wir zunächst $g(n)^{\frac{h}{2}}$. Es gilt:

$$g(n)^{\frac{h}{2}} = (-1)^{b(n)}.$$

$b(n)$ ist genau dann gerade, wenn

$$n \equiv \pm 25^{\frac{b(n)}{2}} \equiv \pm 1(8)$$

ist. Daher gilt also nach [1, Satz 9.10] und [1, Satz 9.9]

$$g(n)^{\frac{h}{2}} = \left(\frac{2}{n}\right), \qquad \text{respektive} \qquad g(n)^h = \left(\frac{2}{n}\right)^2 = \left(\frac{4}{n}\right).$$

Wenden wir uns nun $f(n)$ zu. Mit [1, Satz 9.10] folgt:

$$f(n) = (-1)^{\frac{n-1}{2}} = \left(\frac{-1}{n}\right).$$

Wir erhalten die folgenden vier reellen Dirichlet-Charaktere modulo 2^α:

$$\chi_{1,\frac{h}{2}}(n) = \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right), \quad \chi_{1,h}(n) = \left(\frac{-1}{n}\right)\left(\frac{4}{n}\right), \quad \chi_{2,\frac{h}{2}}(n) = \left(\frac{2}{n}\right), \quad \chi_{2,h}(n) = \left(\frac{4}{n}\right)$$

Dabei ist $\chi_{2,h}$ der triviale Dirichlet-Charakter. Sei nun $\alpha = 2$. Da $\varphi(2^2) = 2$, gibt es genau zwei Charaktere modulo 4. Beide sind reell. Sie sind gegeben durch:

$$\chi_1(n) = \left(\frac{-4}{n}\right) \qquad \text{und} \qquad \chi_2(n) = \left(\frac{4}{n}\right).$$

Dabei ist χ_2 der triviale Dirichlet-Charakter.
Sei nun $\alpha = 1$. Da $\varphi(2) = 1$ ist, ist der einzige Dirichlet-Charakter modulo 2 der triviale Charakter. Auch dieser ist gegeben durch

$$\chi(n) = \left(\frac{4}{n}\right).$$

3. Fall: Sei χ ein reeller, nicht trivialer Dirichlet-Charakter modulo m, wobei $m = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ mit $s, a_1, \dots, a_s \in \mathbb{Z}_{\geq 1}$ ist und $p_1, p_2, \dots, p_s$ Primzahlen sind.
Mit dem chinesischen Restsatz folgt:

$$\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times \cong \left(\frac{\mathbb{Z}}{p_1^{a_1}\mathbb{Z}}\right)^\times \times \left(\frac{\mathbb{Z}}{p_2^{a_2}\mathbb{Z}}\right)^\times \times \dots \times \left(\frac{\mathbb{Z}}{p_s^{a_s}\mathbb{Z}}\right)^\times.$$

Daher können wir χ wie folgt faktorisieren:

$$\chi = \chi_1 \chi_2 \cdots \chi_s,$$

wobei χ_i für $i \in \{1, 2, \dots, s\}$ ein reeller Charakter modulo $p_i^{a_i}$ ist. Die Fälle 1 und 2 zeigen, dass $\chi(n) = \left(\frac{D}{n}\right)$ für ein $D \in \mathbb{Z}$ mit $|D| \leq m^2$. Falls χ ein reeller, nicht trivialer Charakter ist, so folgt, dass mindestens ein χ_i mit $i \in \{1, 2, \dots, s\}$ nicht trivial ist und somit, dass $\chi(n) = \left(\frac{D}{n}\right)$ ist für ein $D \in \mathbb{Z}$, das kein Quadrat ist. □

Lemma 3.16 *Sei $k \in \mathbb{Z}_{\geq 1}$. Für jeden reellen, nicht trivialen Dirichlet-Charakter χ modulo k gibt es ein $x_0 \in \mathbb{R}$, sodass für alle $x > x_0$ gilt:*

$$\sum_{\substack{p \leq x \\ \chi(p)=1}} \frac{\log p}{p} > \frac{1}{9k} \log x.$$

Beweis. Wegen Satz 3.15 ist es ausreichend, die folgende Aussage zu beweisen: Zu jedem $D \in \mathbb{Z}$, das kein Quadrat ist und für das $|D| \leq k^2$ gilt, gibt es ein $x_0 \in \mathbb{R}$ mit

$$\sum_{\substack{p \leq x \\ (\frac{D}{p})=1}} \frac{\log p}{p} > \frac{1}{9k} \log x \text{ für } x > x_0.$$

Definieren wir nun

$$P := \prod_{\substack{|u| < \sqrt{\frac{x}{2}} \\ |v| \leq \sqrt{\frac{x}{2|D|}}}} |u^2 - Dv^2|,$$

wobei der Term $u = v = 0$ weggelassen wird. Dann gelten die folgenden Behauptungen:

Behauptung 1: Sei $C \in \mathbb{R}_{\geq 1}$. Dann gibt es $O(\sqrt{xC})$ viele Terme $(u, v) \in \mathbb{Z}^2$, für die $|u| < \sqrt{\frac{x}{2}}$ und $|v| \leq \sqrt{\frac{x}{2|D|}}$ gilt und

$$|u^2 - Dv^2| \leq C$$

ist.

Beweis. Es gilt:

$$|u^2 - Dv^2| \leq C \Leftrightarrow -C + Dv^2 \leq u^2 \leq C + Dv^2$$

Wenn wir v fixieren, gibt es höchstens $2(\sqrt{2C}+1)$ Werte, die u annehmen kann, damit obige Ungleichungen erfüllt wird. Da $|v| \leq \sqrt{\frac{x}{2|D|}}$ ist, gibt es also höchstens

$$2(\sqrt{2C}+1)(2\sqrt{\frac{x}{2|D|}}) = O(\sqrt{Cx})$$

Paare $(u,v) \in \mathbb{Z}^2$ mit $|u^2 - Dv^2| \leq C$. □

Behauptung 2: Es gilt:

$$\log P \geq \frac{x}{\sqrt{|D|}} \log x + O(x) \tag{3}$$

Beweis. Insgesamt gibt es mindestens

$$4\big(\sqrt{\frac{x}{2}} - 1\big)\big(\sqrt{\frac{x}{2|D|}} - 1\big) = \frac{2x}{\sqrt{|D|}} + O(\sqrt{x})$$

Terme $(u,v) \in \mathbb{Z}^2$ mit $|u| < \sqrt{\frac{x}{2}}$ und $|v| \leq \sqrt{\frac{x}{2|D|}}$. Nach Behauptung 1 ist die Anzahl Terme mit

$$|u^2 - Dv^2| \leq \sqrt{x}$$

gegeben durch $O(x^{\frac{3}{4}})$. Daher gibt es mindestens

$$\frac{2x}{\sqrt{|D|}} + O(x^{\frac{3}{4}})$$

Terme mit

$$|u^2 - Dv^2| > \sqrt{x}$$

Es folgt also:

$$\log P \geq \log\big(x^{\frac{1}{2}(\frac{2x}{\sqrt{|D|}} + O(x^{\frac{3}{4}}))}\big) = \frac{x}{\sqrt{|D|}} \log x + O(x^{\frac{3}{4}} \log x) = \frac{x}{\sqrt{|D|}} \log x + O(x)$$ □

Wir wollen nun für jede Primzahl p die höchste p-Potenz finden, die P teilt. Dazu unterscheiden wir drei Fälle:

1. Fall: Sei $(\frac{D}{p}) = 1$.
Wir versuchen, die Anzahl der Lösungen der Kongruenz

$$u^2 - Dv^2 \equiv 0(p)$$

abzuschätzen. Da $(\frac{D}{p}) = 1$ ist, besitzt die Kongruenz eine Lösung $(u_0, v_0) \in \mathbb{Z}^2$ mit $(u_0, p) = (v_0, p) = 1$. Dann gilt für alle $y, z \in \mathbb{R}$:

$$\begin{aligned}
& \#\{(u,v) \in \mathbb{Z}^2 \mid |u| \leq z, |v| \leq y, u \equiv u_0(p) \text{ und } v \equiv v_0(p)\} \\
= \; & \#\{(u',v') \in \mathbb{Z}^2 \mid |u_0 + pu'| \leq z \text{ und } |v_0 + pv'| \leq y\} \\
= \; & \#\{u' \in \mathbb{Z} \mid -z \leq u_0 + pu' \leq z\} \#\{v' \in \mathbb{Z} \mid -y \leq v_0 + pv' \leq y\} \\
= \; & \#\{u' \in \mathbb{Z} \mid \frac{-z-u_0}{p} \leq u' \leq \frac{z-u_0}{p}\} \#\{v' \in \mathbb{Z} \mid \frac{-y-v_0}{p} \leq v' \leq \frac{y-v_0}{p}\} \\
= \; & \left(\left\lfloor \frac{z-u_0}{p} \right\rfloor - \left\lceil \frac{-z-u_0}{p} \right\rceil + 1\right)\left(\left\lfloor \frac{y-v_0}{p} \right\rfloor - \left\lceil \frac{-y-v_0}{p} \right\rceil + 1\right) \\
= \; & \left(\left\lfloor \frac{z-u_0}{p} \right\rfloor + \left\lfloor \frac{z+u_0}{p} \right\rfloor + 1\right)\left(\left\lfloor \frac{y-v_0}{p} \right\rfloor + \left\lfloor \frac{y+v_0}{p} \right\rfloor + 1\right)
\end{aligned}$$

Wenn wir mit $\sum_{t(p)}$ eine Summe über ein vollständiges Restklassensystem modulo p bezeichnen, erhalten wir:

$$\begin{aligned}
A &:= \#\{(u,v) \in \mathbb{Z}^2 \mid |u| \le z, |v| \le y \text{ und } u^2 - Dv^2 \equiv 0(p)\} \\
&= 2 \cdot \sum_{t(p)} \left(\left\lfloor \frac{z - u_0 t}{p} \right\rfloor + \left\lfloor \frac{z + u_0 t}{p} \right\rfloor + 1 \right) \left(\left\lfloor \frac{y - v_0 t}{p} \right\rfloor + \left\lfloor \frac{y + v_0 t}{p} \right\rfloor + 1 \right) \\
&= 2 \cdot \sum_{t(p)} \frac{2z}{p} \cdot \frac{2y}{p} \\
&\quad + 2 \cdot \sum_{t(p)} \frac{2y}{p} \cdot \left(\left\lfloor \frac{z - u_0 t}{p} \right\rfloor + \left\lfloor \frac{z + u_0 t}{p} \right\rfloor + 1 - \frac{2z}{p} \right) \\
&\quad + 2 \cdot \sum_{t(p)} \frac{2z}{p} \cdot \left(\left\lfloor \frac{y - v_0 t}{p} \right\rfloor + \left\lfloor \frac{y + v_0 t}{p} \right\rfloor + 1 - \frac{2y}{p} \right) \\
&\quad + 2 \cdot \sum_{t(p)} \left(\left\lfloor \frac{z - u_0 t}{p} \right\rfloor + \left\lfloor \frac{z + u_0 t}{p} \right\rfloor + 1 - \frac{2z}{p} \right) \left(\left\lfloor \frac{y - v_0 t}{p} \right\rfloor + \left\lfloor \frac{y + v_0 t}{p} \right\rfloor + 1 - \frac{2y}{p} \right)
\end{aligned}$$

Dabei ist die zweite Zeile gleich:

$$\begin{aligned}
& \frac{4y}{p} \cdot \sum_{t(p)} \left(\left\lfloor \frac{z - u_0 t}{p} \right\rfloor + \left\lfloor \frac{z + u_0 t}{p} \right\rfloor + 1 - \frac{2z}{y} \right) \\
= \; & \frac{4y}{p} \cdot \sum_{s(p)} \left(\left\lfloor \frac{z - s}{p} \right\rfloor + \left\lfloor \frac{z + s}{p} \right\rfloor + 1 - \frac{2z}{p} \right) \\
= \; & \frac{4y}{p} \cdot \left(\sum_{s(p)} \left(\left\lfloor \frac{z - s}{p} \right\rfloor + \left\lfloor \frac{z + s}{p} \right\rfloor \right) + p - 2z \right)
\end{aligned}$$

Sei $\xi := \lfloor z \rfloor$ und $\xi \equiv \sigma(p)$ mit $0 \le \sigma \le p-1$. Das heisst, es gibt ein $k \in \mathbb{Z}$ mit $\xi = \sigma + kp$. Für $0 \le s \le p-1$ erhalten wir:

$$\left\lfloor \frac{z - s}{p} \right\rfloor = \left\lfloor \frac{\xi - s}{p} \right\rfloor = k + \left\lfloor \frac{\sigma - s}{p} \right\rfloor = \begin{cases} \frac{\xi - \sigma}{p}, & \text{wenn } s \le \sigma, \\ \frac{\xi - \sigma}{p} - 1, & \text{wenn } s > \sigma \end{cases}$$

Analog erhält man:

$$\left\lfloor \frac{z + s}{p} \right\rfloor = \left\lfloor \frac{\xi - s}{p} \right\rfloor = k + \left\lfloor \frac{\sigma + s}{p} \right\rfloor = \begin{cases} \frac{\xi - \sigma}{p}, & \text{wenn } s + \sigma < p, \\ \frac{\xi - \sigma}{p} + 1, & \text{wenn } s + \sigma \ge p \end{cases}$$

Es folgt:

$$\begin{aligned}
\sum_{s=0}^{p-1} \left(\left\lfloor \frac{z - s}{p} \right\rfloor + \left\lfloor \frac{z + s}{p} \right\rfloor \right) &= (\sigma+1)\frac{\xi - \sigma}{p} + (p - \sigma - 1)(\frac{\xi - \sigma}{p} - 1) + (p - \sigma)\frac{\xi - \sigma}{p} + \sigma(\frac{\xi - \sigma}{p} + 1) \\
&= 2\xi - p + 1
\end{aligned}$$

Daher ist die zweite Zeile gleich

$$\frac{4y}{p}(2\xi - p + 1 + p - 2z) = \frac{4y}{p}(2\lfloor z \rfloor + 1 - 2z) = O(\frac{y}{p}).$$

Ganz analog folgt, dass die dritte Zeile in $O(\frac{z}{p})$ liegt. Die vierte Zeile lässt sich durch $2p$ nach oben abschätzen. Also erhalten wir zusammengefasst:

$$A \le \frac{8yz}{p} + 2p + O\left(\frac{y}{p}\right) + O\left(\frac{z}{p}\right)$$

Wenn nun $z := \sqrt{\frac{x}{2}}$ und $y := \sqrt{\frac{x}{2|D|}}$, so ist

$$A \leq \frac{4x}{p\sqrt{|D|}} + 2p + O(\frac{\sqrt{x}}{p}) = \frac{4x}{p\sqrt{|D|}} + 2p + O\left(\sqrt{\frac{x}{p}}\right)$$

Das heisst, es werden höchstens

$$\frac{4x}{p\sqrt{|D|}} + 2p + O\left(\sqrt{\frac{x}{p}}\right)$$

Terme $u^2 - Dv^2$ von p geteilt. Sei nun $\alpha \in \mathbb{Z}_{\geq 1}$. Ersetzen wir in der obigen Rechnung p durch p^α, erhalten wir, dass höchstens

$$\frac{4x}{p^\alpha\sqrt{|D|}} + 2p^\alpha + O(\sqrt{\frac{x}{p^\alpha}})$$

Terme $u^2 - Dv^2$ von p^α geteilt werden. In den gegebenen Grenzen von u und v gilt:

$$|u^2 - Dv^2| \leq u^2 + |D|v^2 < \frac{x}{2} + |D|\frac{x}{2|D|} = x.$$

Weiter gilt $p^\alpha < x \Leftrightarrow \alpha < \log_p x$. Daher wird P von einer p-Potenz von höchstens

$$\begin{aligned}
& \sum_{\alpha=1}^{\log_p(x)-1} \left(\frac{4x}{p^\alpha\sqrt{|D|}} + 2p^\alpha + O\left(\sqrt{\frac{x}{p^\alpha}}\right)\right) \\
\leq\ & 2\sum_{\alpha=1}^{\log_p(x)-1} p^\alpha + \sum_{\alpha=1}^{\infty}\left(\frac{4x}{p^\alpha\sqrt{|D|}} + O\left(\sqrt{\frac{x}{p^\alpha}}\right)\right) \\
=\ & 2\frac{x-p}{p-1} + \frac{4x}{(p-1)\sqrt{|D|}} + O\left(\sqrt{\frac{x}{p}}\right) \\
\leq\ & \frac{4x}{p\sqrt{|D|}} + \frac{4}{p(p-1)}\frac{x}{\sqrt{|D|}} + \frac{2x}{p} + \frac{2x}{p(p-1)} + O\left(\sqrt{\frac{x}{p}}\right) \\
=\ & \frac{4x}{p\sqrt{|D|}} + \frac{2x}{p} + O\left(\sqrt{\frac{x}{p}}\right) + O\left(\frac{x}{p^2}\right)
\end{aligned}$$

geteilt.

2.Fall: Sei $(\frac{D}{p}) = -1$.
Damit p^α $u^2 - Dv^2$ teilt, muss p^α sowohl u als auch v teilen. Daher gibt es höchstens $O(\frac{x}{p^{2\alpha}})$ viele Paare (u, v), die Lösungen von $u^2 - Dv^2 \equiv 0(p^\alpha)$ sind. Daher wird P von einer p-Potenz von höchstens

$$O\left(x\sum_{\alpha=1}^{\infty}\frac{1}{p^{2\alpha}}\right) = O\left(\frac{x}{p^2-1}\right) \subset O\left(\frac{x}{p^2}\right)$$

geteilt.

3.Fall: Sei $(\frac{D}{p}) = 0$.
In diesem Fall ist D ein Vielfaches von p. Das heisst, P wird von einer p-Potenz von höchstens

$$O\left(\sum_{\alpha=1}^{\infty}\frac{2\sqrt{\frac{x}{2|D|}}2\sqrt{\frac{x}{2}}}{p^{2\alpha-1}}\right) = O\left(\frac{2xp}{\sqrt{|D|}}\frac{1}{p^2-1}\right) \subset O\left(\frac{x}{p}\right)$$

geteilt.

Zusammengefasst ergeben die obigen drei Fälle:

$$\log P \leq \left(4\frac{x}{\sqrt{|D|}}+2x\right)\sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O\left(\sqrt{x}\sum_{p\leq x}\frac{\log p}{\sqrt{p}}\right)+O\left(x\sum_{p\leq x}\frac{\log p}{p^2}\right)+O\left(x\sum_{p|D}\frac{\log p}{p}\right)$$
$$=\left(4\frac{x}{\sqrt{|D|}}+2x\right)\sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O(x). \quad (4)$$

Die O-Terme wurden dabei wie folgt abgeschätzt: Beim ersten O-Term verwenden wir Satz 2.11 und Satz 2.7 mit

$$a(n):=\begin{cases}\frac{\log n}{n}, & \text{wenn } n \text{ prim ist}\\ 0 & \text{sonst}\end{cases} \quad \text{und } f(t):=\sqrt{t}.$$

Beim zweiten O-Term verwenden wir Satz 2.7 mit $a(n)$ definiert wie oben und $f(t):=\frac{1}{t}$ zusammen mit Satz 2.11. Wenn wir das Resultat in (4) mit (3) vergleichen, erhalten wir:

$$\frac{x}{\sqrt{|D|}}\log x \leq \left(\frac{4x}{\sqrt{|D|}}+2x\right)\sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O(x)\leq 6x\sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O(x)$$
$$\Rightarrow \frac{1}{6\sqrt{|D|}}\log x \leq \sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O(1).$$

Und da $|D|\leq k^2$ ist, folgt

$$\frac{1}{7k}\log x < \sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}+O(1),$$

respektive gibt es ein $x_0\in\mathbb{R}$ mit

$$\sum_{\substack{p\leq x\\(\frac{D}{p})=1}}\frac{\log p}{p}>\frac{1}{9k}\log x$$

für alle $x>x_0$. □

4 Selbergs Beweis des Dirichletschen Primzahlsatzes

4.1 Notationen

Für festes k verwenden wir im Folgenden diese Notationen:

$$S_l(x):=\sum_{\substack{p\leq x\\p\equiv l(k)}}\frac{\log p}{p} \qquad Q_l(x):=\frac{S_l(x)}{\log x}.$$

Des weiteren seien

$$\lambda_d=\lambda_{d,x}:=\mu(d)\log^2\frac{x}{d}$$

und

$$\theta_n=\theta_{n,x}:=\sum_{d|n}\lambda_d.$$

4.2 Ungleichungen für $Q_l(x)$

Lemma 4.1 *Seien $n \in \mathbb{Z}_{\geq 1}$ und $x \in \mathbb{R}$. Dann gilt:*

$$\theta_n = \begin{cases} \log^2 x, & \text{wenn } n = 1, \\ \log p \log \frac{x^2}{p}, & \text{wenn } n = p^\alpha, \alpha \geq 1, \\ 2 \log p \log q, & \text{wenn } n = p^\alpha q^\beta, p \neq q, \alpha \geq 1, \beta \geq 1, \\ 0 & \text{sonst.} \end{cases}$$

Beweis. ***1.Fall*** : $n = 1$
Da $\mu(1) = 1$ ist, erhalten wir: $\theta_1 = \lambda_1 = \mu(1) \log^2 x = \log^2 x$.

2.Fall : $n = p^\alpha, \alpha \geq 1$
Es gilt $\mu(p^\alpha) = 0$ für alle $\alpha \geq 2$. Daher erhalten wir:

$$\begin{aligned} \theta_{p^\alpha} = \mu(1) \log^2 x + \mu(p) \log^2 \frac{x}{p} &= \log^2 x - (\log x - \log p)^2 \\ &= 2 \log x \log p - \log^2 p = \log p (2 \log x - \log p) = \log p \log \frac{x^2}{p}. \end{aligned}$$ □

3.Fall : $n = p^\alpha q^\beta, \alpha \geq 1, \beta \geq 1$
Mit derselben Beobachtung wie in Fall 2 erhalten wir:

$$\begin{aligned} \theta_{p^\alpha q^\beta} &= \mu(1) \log^2 x + \mu(p) \log^2 \frac{x}{p} + \mu(q) \log^2 \frac{x}{q} + \mu(pq) \log^2 \frac{x}{pq} \\ &= \log^2 x - \log^2 \frac{x}{p} - \log^2 \frac{x}{q} + \log^2 \frac{x}{pq} \\ &= \log^2 x - (\log x - \log p)^2 - (\log x - \log q)^2 + (\log x - \log q - \log p)^2 \\ &= 2 \log p \log q. \end{aligned}$$

4.Fall : n nicht wie in den Fällen 1-3.
Dieser Fall folgt induktiv. Dabei reicht es, den Fall zu betrachen, in dem n quadratfrei ist. Denn falls $d \mid n$ und d durch ein Quadrat teilbar ist, so folgt $\mu(d) = 0$. Sei $i \in \mathbb{Z}_{\geq 2}$. Dann gilt für $n = p_1 p_2 \dots p_i$:

$$\theta_{p_1 p_2 \dots p_i, x} = \theta_{p_1 p_2 \dots p_{i-1}, x} - \theta_{p_1 p_2 \dots p_{i-1}, \frac{x}{p_i}},$$

denn

$$\begin{aligned} \theta_{p_1 p_2 \dots p_{i-1}, x} - \theta_{p_1 p_2 \dots p_{i-1}, \frac{x}{p_i}} &= \sum_{d \mid \frac{n}{p_i}} \mu(d) \log^2 \frac{x}{d} - \sum_{d \mid \frac{n}{p_i}} \mu(d) \log^2 \frac{x}{p_i d} \\ &= \sum_{d \mid \frac{n}{p_i}} \mu(d) \log^2 \frac{x}{d} + \sum_{d \mid \frac{n}{p_i}} \mu(d p_i) \log^2 \frac{x}{p_i d} \\ &= \sum_{d \mid n, p_i \nmid d} \mu(d) \log^2 \frac{x}{d} + \sum_{d \mid n, p_i \mid d} \mu(d) \log^2 \frac{x}{d} \\ &= \sum_{d \mid n} \mu(d) \log^2 \frac{x}{d} = \theta_n. \end{aligned}$$

Lemma 4.2 *Für alle $x \in \mathbb{R}$ und alle teilerfremden $k, l \in \mathbb{Z}_{\geq 1}$ gilt:*

$$\sum_{\substack{p \leq x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \leq x \\ pq \equiv l(k)}} \log p \log q = \frac{x}{k} \sum_{\substack{d \leq x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(x). \tag{5}$$

Dabei sind p und q verschiedene Primzahlen.

Beweis. Wir wollen die Summe $\sum_{\substack{n\leq x\\ n\equiv l(k)}} \theta_n$ auf zwei verschiedene Arten abschätzen. Daraus können wir anschliessend (5) herleiten. Die erste Abschätzung erhalten wir mit Lemma 4.1 wie folgt:

$$\sum_{\substack{n\leq x\\ n\equiv l(k)}} \theta_n = \sum_{\substack{p^\alpha\leq x\\ p^\alpha\equiv l(k)}} \log p \log\frac{x^2}{p} + \sum_{\substack{p^\alpha q^\beta\leq x\\ p^\alpha q^\beta\equiv l(k)}} \log p\log q + O(\log^2 x). \tag{6}$$

Dabei sind p und q verschieden. Den Faktor 2 vor der zweiten Summe dürfen wir weglassen, wenn wir $p^\alpha q^\beta$ und $q^\beta p^\alpha$ als verschieden betrachten. Daher gilt:

$$\begin{aligned}
\sum_{\substack{n\leq x\\ n\equiv l(k)}} \theta_n &= \sum_{\substack{p\leq x\\ p\equiv l(k)}} \log p\log\frac{x^2}{p} + O(2\log x\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p) + \sum_{\substack{p^\alpha q^\beta\leq x\\ p^\alpha q^\beta\equiv l(k)}}\log p\log q + O(\log^2 x)\\
&= \sum_{\substack{p\leq x\\ p\equiv l(k)}}\log^2 p + 2\sum_{\substack{p\leq x\\ p\equiv l(k)}}\log p\log\frac{x}{p} + O(\log x\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p) + \sum_{\substack{pq\leq x\\ pq\equiv l(k)}}\log p\log q\\
&\qquad + (\sum_{\substack{p^\alpha q^\beta\leq x\\ \alpha\geq 2}}\log p\log q) + O(\log^2 x)\\
&= \sum_{\substack{p\leq x\\ p\equiv l(k)}}\log^2 p + \sum_{\substack{pq\leq x\\ pq\equiv l(k)}}\log p\log q + O\Big(\sum_{\substack{p\leq x\\ p\equiv l(k)}}\log p\log\frac{x}{p}\Big) + O(\log x\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p)\\
&\qquad + O(\sum_{\substack{p^\alpha q^\beta\leq x\\ \alpha\geq 2}}\log p\log q) + O(\log^2 x)\\
&= \sum_{\substack{p\leq x\\ p\equiv l(k)}}\log^2 p + \sum_{\substack{pq\leq x\\ pq\equiv l(k)}}\log p\log q + O(x).
\end{aligned} \tag{7}$$

Die O-Terme wurden dabei wie folgt abgeschätzt:

$$O(\log x\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p)\subset O(\log x\sum_{p\leq\sqrt{x}}\sum_{\alpha\leq\frac{\log x}{\log p}}\log p)\subset O(\sqrt{x}\log x)\subset O(x),$$

wobei Satz 2.8 verwendet wurde. Mit Hilfe desselben Satzes und der geometrischen Reihe erhalten wir:

$$\begin{aligned}
O(\sum_{\substack{p^\alpha q^\beta\leq x\\ \alpha\geq 2}}\log p\log q) &= O(\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p\sum_{q\leq\frac{x}{p^\alpha}}\sum_{\beta\leq\frac{\log\frac{x}{p^\alpha}}{\log q}}\log q)\\
&\subset O\Big(\sum_{\substack{p^\alpha\leq x\\ \alpha\geq 2}}\log p\sum_{q\leq\frac{x}{p^\alpha}}\log\frac{x}{p^\alpha}\Big)\\
&\subset O(\sum_{\substack{p^\alpha\leq x\\ \alpha\leq 2}}\log p\frac{x}{p^\alpha})\\
&\subset O(x\sum_{p\leq\sqrt{x}}\log p\sum_{\alpha=2}^{\infty}\Big(\frac{1}{p}\Big)^\alpha)\\
&= O(x\sum_{p\leq\sqrt{x}}\frac{1}{p(p-1)}\log p)\\
&\subset O\Big(x\sum_{n=2}^{\infty}\frac{\log n}{(n-1)^2}\Big)\\
&= O(x),
\end{aligned}$$

weil $\sum_{n=2}^{\infty} \frac{\log n}{(n-1)^2} < \infty$ ist. Mittels Satz 2.11 und Satz 2.7, wobei wir

$$f(t) := t \log \frac{x}{t} \qquad \text{und} \qquad a(n) := \begin{cases} \frac{\log n}{n}, & \text{wenn } n \text{ prim} \\ 0 & \text{sonst.} \end{cases}$$

wählen, können wir auch den letzten O-Term abschätzen:

$$\sum_{p \le x} \log p \log \frac{x}{p} = \int_1^x \left(\sum_{p \le t} \frac{\log p}{p} \right) \left(1 - \log \frac{x}{t} \right) dt$$
$$= \int_1^x \{\log t + O(1)\} \left(1 - \log \frac{x}{t} \right) dt = x \log x - x \log x + O(x) = O(x).$$

Kommen wir nun zur zweiten Abschätzung der Summe $\sum_{\substack{n \le x \\ n \equiv l(k)}} \theta_n$. Hier benutzen wir direkt die Definition von θ_n.

$$\sum_{\substack{n \le x \\ n \equiv l(k)}} \theta_n = \sum_{\substack{n \le x \\ n \equiv l(k)}} \sum_{d \mid n} \lambda_d = \sum_{\substack{d \le x \\ (d,k)=1}} \lambda_d \sum_{\substack{d \mid n \\ n \le x, n \equiv l(k)}} 1 = \frac{x}{k} \sum_{\substack{d \le x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(\sum_{d \le x} |\lambda_d|)$$
$$= \frac{x}{k} \sum_{\substack{d \le x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(x), \quad (8)$$

wobei der O-Term mit Satz 2.7 und $|\mu(d)| \le 1$ wie folgt abgeschätzt wurde:

$$\sum_{d \le x} |\lambda_d| \le \sum_{d \le x} \log^2 \frac{x}{d} = 2 \int_1^x \left(\sum_{d \le t} 1 \right) \frac{\log \frac{x}{t}}{t} dt + O(\log^2 x)$$
$$\le 2 \int_1^x \log \frac{x}{t} dt + O(\log^2 x) = O(x).$$

Nun können wir (7) und (8) gleichsetzen und erhalten:

$$\sum_{\substack{p \le x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \le x \\ pq \equiv l(k)}} \log p \log q = \frac{x}{k} \sum_{\substack{d \le x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(x). \qquad \square$$

Lemma 4.3 *Ist $(l,k) > 1$, so ist die linke Seite von (5) in O(x).*

Beweis. Nehmen wir an, dass $(l,k) > 1$ ist. Wenn wir mit $\mathbb{P}$ die Menge aller Primzahlen bezeichnen gilt:

$$\sum_{\substack{p \le x \\ p \equiv l(k)}} \log^2 p \le \begin{cases} 0, & \text{wenn } (l,k) \notin \mathbb{P}, \\ \log^2 r, & \text{wenn } (l,k) = r \in \mathbb{P}. \end{cases}$$

Wenn nun (l,k) einen Primfaktor r hat und

$$pq \equiv l(k)$$

ist, so gibt es ein $n \in \mathbb{Z}$ mit

$$pq = l + nk.$$

Definieren wir $l' := \frac{l}{r} \in \mathbb{Z}_{\ge 1}$ und $k' := \frac{k}{r} \in \mathbb{Z}_{\ge 1}$, so haben wir:

$$pq = rl' + nrk' \Rightarrow r \mid pq \Rightarrow r \mid p \text{ oder } r \mid q.$$

Da p und q Primzahlen sind, folgt also $p = r$ oder $q = r$. OBdA sei $p = r$. Der andere Fall folgt nach Vertauschung der Rollen von p und q. Folglich erhalten wir mit Satz 2.8:

$$\sum_{\substack{pq\le x\\ pq\equiv l(k)}} \log p \log q \le \log r \sum_{\substack{q\le \frac{x}{r}\\ q\equiv l'(k')}} \log q \le \log r \log \frac{x}{r} \sum_{q\le \frac{x}{r}} 1 = O\left(\frac{\log r}{r} x\right) \subset O(x).$$

Also ist die linke Seite aus (5) in $O(x)$. □

Lemma 4.4 *Es gilt:*

$$A_l(x) := \sum_{\substack{p\le x\\ p\equiv l(k)}} \frac{\log^2 p}{p} + \sum_{\substack{pq\le x\\ pq\equiv l(k)}} \frac{\log p \log q}{pq} = \frac{1}{\varphi(k)} \log^2 x + O(\log x).$$

Beweis. Definiere

$$K_l(x) := \sum_{\substack{p\le x\\ p\equiv l(k)}} \log^2 p + \sum_{\substack{pq\le x\\ pq\equiv l(k)}} \log p \log q$$

und

$$T_l(x) := \sum_{\substack{p\le x\\ p\equiv l(k)}} \frac{\log^2 p}{p} + \sum_{\substack{pq\le x\\ pq\equiv l(k)}} \frac{\log p \log q}{pq}.$$

Aus Lemma 4.3 zusammen mit (5) erhalten wir:

$$\begin{aligned}\sum_{0\le l'<k} K_{l'} = \sum_{\substack{0\le l<k\\ (l,k)=1}} K_{l'} + O(x) &= \sum_{\substack{0\le l<k\\ (l,k)=1}} \left(\frac{x}{k} \sum_{\substack{d\le x\\ (d,k)=1}} \frac{\lambda_d}{d} + O(x)\right)\\ &= \varphi(k)\left(\frac{x}{k} \sum_{\substack{d\le x\\ (d,k)=1}} \frac{\lambda_d}{d} + O(x)\right) = \varphi(k) K_l + O(x)\end{aligned}$$

Nach Division durch $\varphi(k)$ erhalten wir:

$$K_l(x) = \frac{1}{\varphi(k)} \left\{ \sum_{0\le l'<k} K_{l'}(x) \right\} + O(x).$$

Mit Satz 2.7 folgt:

$$T_l(x) = \frac{1}{x} K_l(x) + \int_1^x K_l(t) \frac{1}{t^2} dt + O(1).$$

Also

$$\begin{aligned}T_l(x) - \frac{1}{\varphi(k)} \sum_{0\le l'<k} T_{l'}(x) &= \frac{1}{x} K_l(x) + \int_1^x K_l(t) \frac{1}{t^2} dt + O(1)\\ &\quad - \frac{1}{\varphi(k)} \sum_{0\le l'<k} \left\{ \frac{1}{x} K_{l'}(x) + \int_1^x K_{l'}(t) \frac{1}{t^2} dt + O(1) \right\}\\ &= \frac{1}{x}\left\{ K_l(x) - \frac{1}{\varphi(k)} \sum_{0\le l'<k} K_{l'}(x) \right\} + \int_1^x \left\{ K_l(t) - \frac{1}{\varphi(k)} \sum_{0\le l'<k} K_l'(t) \right\} \frac{1}{t^2} dt + O(1)\\ &= \frac{1}{x} O(x) + O\left(\int_1^x t \frac{1}{t^2} dt \right) = O(\log x).\end{aligned}$$

Daraus folgt das Lemma. □

Lemma 4.5 *Für alle $x \in \mathbb{R}$ gilt:*

$$\sum_{\substack{p\le x\\ p\equiv l(k)}} \frac{\log^3 p}{p} + 2 \sum_{\substack{pq\le x\\ pq\equiv l(k)}} \frac{\log p \log^2 q}{pq} = \frac{2}{3\varphi(k)} \log^3 x + O(\log^2 x). \tag{9}$$

Beweis. Sei A_l definiert wie in Lemma 4.4. Dann erhalten wir mit Satz 2.7 und Lemma 4.4:

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv l(k)}}\frac{\log^3 p}{p}+\sum_{\substack{pq\le x\\ p\equiv l(k)}}\frac{\log p\log q}{pq}\log pq &= A_l(x)\log x-\int_1^x A_l(t)\frac{1}{t}dt\\ &=\{\frac{1}{\varphi(k)}\log^2 x+O(\log x)\}\log x-\int_1^x\{\frac{1}{\varphi(k)}\log^2 t+O(\log t)\}\frac{1}{t}dt\\ &=\frac{2}{3\varphi(k)}\log^3 x+O(\log^2 x).\end{aligned}$$

Da $\log pq=\log p+\log q$ ist, folgt das Lemma. □

Lemma 4.6 *Für alle teilerfremden $l,k\in\mathbb{Z}_{\ge 1}$ gelten:*

1. *Es gibt ein $x_0\in\mathbb{R}$, sodass für alle $x>x_0$ gilt:*

$$Q_l(x)>\frac{1}{10\varphi(k)}-\frac{1}{9}\sum_{mm'\equiv l(k)}Q_m(x^{\frac{1}{3}})Q_{m'}(x^{\frac{1}{3}}). \tag{10}$$

2. *Für alle $x\in\mathbb{R}$ gilt:*

$$Q_l(x)\ge\frac{2}{27}\sum_{mm'm''\equiv l(k)}Q_m(x^{\frac{1}{3}})Q_{m'}(x^{\frac{1}{3}})Q_{m''}(x^{\frac{1}{3}})+O\Big(\frac{1}{\log x}\Big) \tag{11}$$

3. *Für alle $x\in\mathbb{R}$ gilt:*

$$Q_l(x)\le\frac{2}{\varphi(k)}+O\Big(\frac{\log\log x}{\log x}\Big). \tag{12}$$

Beweis. Wir definieren nun $\bar p$ so, dass $p\bar p\equiv 1(k)$ ist. Dann erhalten wir mit Lemma 4.4:

$$\begin{aligned}\sum_{\substack{pq\le x\\ pq\equiv l(k)}}\frac{\log p\log^2 q}{pq}&=\sum_{p\le x}\frac{\log p}{p}\sum_{\substack{q\le\frac{x}{p}\\ q\equiv l\bar p(k)}}\frac{\log^2 q}{q}\\ &=\frac{1}{\varphi(k)}\sum_{p\le x}\frac{\log p}{p}\log^2\frac{x}{p}-\sum_{p\le x}\frac{\log p}{p}\sum_{\substack{qr\le\frac{x}{p}\\ qr\equiv l\bar p(k)}}\frac{\log q\log r}{qr}+O\Big(\sum_{p\le x}\frac{\log p}{p}\log x\Big)\\ &=-\sum_{\substack{pqr\le x\\ pqr\equiv l(k)}}\frac{\log p\log q\log r}{pqr}+\frac{1}{3\varphi(k)}\log^3 x+O(\log^2 x),\end{aligned} \tag{13}$$

wobei wir den O-Term mittels Satz 2.11 abgeschätzt haben und verwendet haben, dass

$$\begin{aligned}\sum_{p\le x}\frac{\log p}{p}\log^2\frac{x}{p}&=\log^2 x\sum_{p\le x}\frac{\log p}{p}-2\log x\sum_{p\le x}\frac{\log^2 p}{p}+\sum_{p\le x}\frac{\log^3 p}{p}\\ &=\log^2 x\{\log x+O(1)\}-2\log x\{\frac{1}{2}\log^2 x+O(\log x)\}+\{\frac{1}{3}\log^3 x+O(\log^2 x)\}\\ &=\frac{1}{3}\log^3 x+O(\log^2 x)\end{aligned}$$

mit Korollar 2.12 folgt. Setzen wir nun (13) in (9) ein, so erhalten wir:

$$\sum_{\substack{p\le x\\ p\equiv l(k)}}\frac{\log^3 p}{p}=2\sum_{\substack{pqr\le x\\ pqr\equiv l(k)}}\frac{\log p\log q\log r}{pqr}+O(\log^2 x). \tag{14}$$

Wieder aus Lemma 4.4 können wir folgern:

$$\sum_{\substack{p\le x\\ p\equiv l(k)}}\frac{\log^2 p}{p}\le\frac{1}{\varphi(k)}\log^2 x+O(\log x).$$

Mit Satz 2.7 erhalten wir daraus:

$$\sum_{\substack{p\leq x\\ p\equiv l(k)}}\frac{\log p}{p}=\Big(\sum_{\substack{p\leq x\\ p\equiv l(k)}}\frac{\log^2 p}{p}\Big)\frac{1}{\log x}+\int_2^x\Big(\sum_{\substack{p\leq t\\ p\equiv l(k)}}\frac{\log^2 p}{p}\Big)\frac{1}{t\log^2 t}dt+O(1)$$
$$\leq\Big\{\frac{1}{\varphi(k)}\log^2 x+O(\log x)\Big\}\frac{1}{\log x}+\int_2^x\Big\{\frac{1}{\varphi(k)}\log^2 t+O(\log t)\Big\}\frac{1}{t\log^2 t}dt$$
$$=\frac{2\log x}{\varphi(k)}+O(\log\log x)\quad(15)$$

Mit (15) erhalten wir also:

$$\sum_{\substack{pq\leq x\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}=\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}+\sum_{p\leq x^{\frac13}}\sum_{\substack{x^{\frac13}<q\leq\frac{x}{p}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}$$
$$+\sum_{x^{\frac13}<p\leq x}\sum_{\substack{q\leq\frac{x}{p}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}$$
$$\leq\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}+2\sum_{x^{\frac13}<p\leq x}\frac{\log p}{p}\sum_{\substack{q\leq\frac{x}{p}\\ q\equiv l\bar{p}(k)}}\frac{\log q}{q}$$

$$\leq\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}+\frac{4}{\varphi(k)}\sum_{x^{\frac13}<p\leq x}\frac{\log p}{p}\log\frac{x}{p}+O(\log\log x\sum_{p\leq x}\frac{\log p}{p})$$
$$=\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}+\frac{8}{9\varphi(k)}\log^2 x+O(\log\log x\log x),\quad(16)$$

wobei wir den O-Term mit Satz 2.11 abgeschätzt haben und die folgende Formel verwendet haben, die mit Korollar 2.12 hergeleitet wird:

$$\sum_{x^{\frac13}<p\leq x}\frac{\log p}{p}\log\frac{x}{p}=\log x\sum_{x^{\frac13}<p\leq x}\frac{\log p}{p}-\sum_{x^{\frac13}<p\leq x}\frac{\log^2 p}{p}$$
$$=\log x\{\log x-\frac13\log x+O(1)\}-\{\frac12\log^2 x-\frac{1}{18}\log^2 x+O(\log x)\}$$
$$=\frac29\log^2 x+O(\log x).$$

Setzen wir (16) nun in die Formel aus Lemma 4.4 ein, erhalten wir:

$$\sum_{\substack{p\leq x\\ p\equiv l(k)}}\frac{\log^2 p}{p}\geq\frac{1}{9\varphi(k)}\log^2 x-\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}+O(\log x\log\log x),$$

oder, wenn $x>x_0$, für ein genügend grosses $x_0\in\mathbb{R}$:

$$\log x\sum_{\substack{p\leq x\\ p\equiv l(k)}}\frac{\log p}{p}>\frac{1}{10\varphi(k)}\log^2 x-\sum_{p\leq x^{\frac13}}\sum_{\substack{q\leq x^{\frac13}\\ pq\equiv l(k)}}\frac{\log p\log q}{pq},$$

also auch für alle $x>x_0$:

$$\log x S_l(x)>\frac{1}{10\varphi(k)}\log^2 x-\sum_{mm'\equiv l(k)}S_m(x^{\frac13})S_{m'}(x^{\frac13}).$$

Dividieren wir obige Formel durch $\log^2 x$ so erhalten wir

$$Q_l(x) > \frac{1}{10\varphi(k)} - \frac{1}{9} \sum_{mm' \equiv l(k)} Q_m(x^{\frac{1}{3}}) Q_{m'}(x^{\frac{1}{3}}),$$

für alle $x > x_0$. Weiter gilt:

$$2 \sum_{\substack{pqr \leq x \\ pqr \equiv l(k)}} \frac{\log p \log q \log r}{pqr} \geq 2 \sum_{p \leq x^{\frac{1}{3}}} \sum_{\substack{q \leq x^{\frac{1}{3}} \\ pqr \equiv l(k)}} \sum_{r \leq x^{\frac{1}{3}}} \frac{\log p}{p} \frac{\log q}{q} \frac{\log r}{r}$$

$$= 2 \sum_{mm'm'' \equiv l(k)} S_m(x^{\frac{1}{3}}) S_{m'}(x^{\frac{1}{3}}) S_{m''}(x^{\frac{1}{3}}).$$

Der letzte Term ist nach Division durch $\log^3 x$ gegeben durch:

$$\frac{2}{27} \sum_{mm'm'' \equiv l(k)} Q_m(x^{\frac{1}{3}}) Q_{m'}(x^{\frac{1}{3}}) Q_{m''}(x^{\frac{1}{3}}).$$

Nach (14) gilt folglich:

$$\log^2 x \sum_{\substack{p \leq x \\ p \equiv l(k)}} \frac{\log p}{p} \geq \sum_{\substack{p \leq x \\ p \equiv l(k)}} \frac{\log^3 p}{p} = 2 \sum_{\substack{pqr \leq x \\ pqr \equiv l(k)}} \frac{\log p \log q \log r}{pqr} + O(\log^2 x).$$

Also erhalten wir nach Division durch $\log^3 x$, dass

$$Q_l(x) \geq \frac{2}{27} \sum_{mm'm'' \equiv l(k)} Q_m(x^{\frac{1}{3}}) Q_{m'}(x^{\frac{1}{3}}) Q_{m''}(x^{\frac{1}{3}}) + O\left(\frac{1}{\log x}\right)$$

ist. Aus (15) erhalten wir nach Division durch $\log x$:

$$Q_l(x) \leq \frac{2}{\varphi(k)} + O\left(\frac{\log \log x}{\log x}\right). \qquad \square$$

4.3 Beweis von Satz 1.2

In diesem Abschnitt können wir annehmen, dass $\varphi(k) \geq 2$. Denn $\varphi(k) = 1$ genau dann wenn $k = 1$ oder $k = 2$ ist. Für diese Fälle folgt der Dirichletsche Primzahlsatz aus der Tatsache, dass es unendlich viele Primzahlen gibt.[1]
Nun können wir Satz 1.2 beweisen. Wir werden zeigen, dass es ein $x_0 \in \mathbb{R}$ gibt mit:

$$Q_l(x) > \frac{1}{20^4 (\varphi(k))^3 k^3}$$

für alle $x > x_0$. Nehmen wir an, dass

$$Q_l(x) < \frac{1}{30\varphi(k)} \tag{17}$$

ist für alle genügend grossen $x \in \mathbb{R}$. Aus Satz 2.11 folgt:

$$\sum_{0 \leq n < k} \sum_{\substack{p \leq x^{\frac{1}{3}} \\ p \equiv n(k)}} \frac{\log p}{p} = \sum_{p \leq x^{\frac{1}{3}}} \frac{\log p}{p} = \log x^{\frac{1}{3}} + O(1). \Rightarrow \sum_{0 \leq n < k} Q_n(x^{\frac{1}{3}}) = 1 + O\left(\frac{1}{\log x}\right). \tag{18}$$

[1] Vier verschiedene Beweise, dass es unendlich viele Primzahlen gibt, kann man in [6] auf den Seiten 2, 28, 34 und 95 finden.

Angenommen, für mehr als $\frac{1}{2}\varphi(k)$ Werte von m gilt

$$Q_m(x^{\frac{1}{3}}) \leq \frac{1}{20(\varphi(k))^2}.$$

Dann folgt mit (12) und (18):

$$\begin{aligned} 1+O\left(\frac{1}{\log x}\right) = \sum_n Q_n(x^{\frac{1}{3}}) &\leq (\frac{1}{2}\varphi(k)+1)\frac{1}{20(\varphi(k))^2} + (\frac{1}{2}\varphi(k)-1)\left(\frac{2}{\varphi(k)} + O\left(\frac{\log\log x}{\log x}\right)\right) \\ &= \frac{-79\varphi(k)+2}{40(\varphi(k))^2} + 1 + O\left(\frac{\log\log x}{\log x}\right). \end{aligned}$$

Da der erste Term auf der rechten Seite kleiner als Null ist, haben wir einen Widerspruch, wenn $x > x_0$ für ein $x_0 \in \mathbb{R}$ gross genug. Daher gibt es mindestens $\frac{1}{2}\varphi(k)$ Werte m mit

$$Q_m(x^{\frac{1}{3}}) > \frac{1}{20(\varphi(k))^2} \text{ für } x > x_0.$$

Aus Lemma 3.16 erhalten wir für jeden reellen, nicht trivialen Dirichlet-Charakter χ modulo k, dass

$$\sum_{\chi(n)=1} Q_n(x^{\frac{1}{3}}) > \frac{1}{9k}$$

ist für alle $x > x_0$. Daher gibt es mindestens ein m mit

$$Q_m(x^{\frac{1}{3}}) > \frac{1}{2}\frac{1}{9\varphi(k)k}$$

und $\chi(\hat{m}) = 1$, denn sonst wäre

$$\sum_{\chi(n)=1} Q_n(x^{\frac{1}{3}}) \leq \varphi(k)\frac{1}{2}\frac{1}{9\varphi(k)k} < \frac{1}{9k}.$$

Des weiteren erhalten wir aus (10) und (17), dass

$$\sum_{nn'\equiv l(k)} Q_n(x^{\frac{1}{3}})Q_{n'}(x^{\frac{1}{3}}) > \frac{1}{15\varphi(k)} \tag{19}$$

ist für alle $x > x_0$. Hier stellt sich die Frage, wie viele Paare von ganzen Zahlen (n, n') mit $0 \leq n, n' < k$ es gibt mit $(n, k) = 1 = (n', k)$ und $nn' \equiv l(k)$. Mit Lemma 3.7 folgt, dass wenn n fest gewählt wurde, es bis auf Kongruenz modulo k höchstens ein n' gibt. Falls tatsächlich ein solches n' existiert, so folgt wegen der Bedingung $n' \leq k$ Eindeutigkeit. Das heisst, es gibt höchstens $\varphi(k)$ solche Paare (n, n').

Angenommen für alle diese Paare (n, n') gilt

$$Q_n(x^{\frac{1}{3}})Q_{n'}(x^{\frac{1}{3}}) \leq \frac{1}{15(\varphi(k))^2}$$

für alle genügend grossen $x \in \mathbb{R}$. Dann folgt

$$\sum_{nn'\equiv l(k)} Q_n(x^{\frac{1}{3}})Q'_n(x^{\frac{1}{3}}) \leq \frac{1}{15\varphi(k)}$$

für alle genügend grossen $x \in \mathbb{R}$ im Widerspruch zu (19). Das heisst, es gibt mindestens ein Paar (m, m') mit $mm' \equiv l(k)$ und

$$Q_m(x^{\frac{1}{3}})Q_{m'}(x^{\frac{1}{3}}) > \frac{1}{15(\varphi(k))^2}, \tag{20}$$

respektive, da $\varphi(k) \geq 2$,

$$Q_m(x^{\frac{1}{3}}) > \frac{1}{31\varphi(k)} > \frac{1}{20(\varphi(k))^2} \qquad \text{und} \qquad Q_{m'}(x^{\frac{1}{3}}) > \frac{1}{20(\varphi(k))^2}.$$

Von diesen beiden Ungleichungen wollen wir die erste herleiten. Die zweite folgt dann analog nach Vertauschung der Rolle von m und m'. Angenommen

$$Q_m(x^{\frac{1}{3}}) \leq \frac{1}{31\varphi(k)}.$$

Mit (12) und (20) folgt

$$\frac{1}{15(\varphi(k))^2} < Q_m(x^{\frac{1}{3}})Q_{m'}(x^{\frac{1}{3}}) \leq \frac{1}{31\varphi(k)}\left(\frac{2}{\varphi(k)} + O\left(\frac{\log\log x}{\log x}\right)\right)$$
$$= \frac{1}{15.5(\varphi(k))^2} + O\left(\frac{\log\log x}{\log x}\right).$$

Dies ist ein Widerspruch für genügend grosses x.
Zusammengefasst können wir also h Repräsentanten von paarweise verschiedenen Restklassen modulo k finden mit $h \geq \frac{1}{2}(\varphi(k))$ und

$$Q_{m_i}(x^{\frac{1}{3}}) > \frac{1}{20\varphi(k)k},$$

wobei $i = 1, 2, \ldots, h$. Weiter gibt es zu jedem reellen Charakter χ ein $m_i \in \{m_1, m_2, \ldots m_h\}$ mit $\chi(\hat{m_i}) = 1$ und es gibt $m, m' \in \{m_1, m_2, \ldots m_h\}$ mit $mm' \equiv l(k)$. Daher können wir Lemma 3.9 anwenden und schliessen, dass es $m, m', m'' \in \{m_1, m_2, \ldots m_h\}$ gibt mit $mm'm'' \equiv l(k)$. Aus (11) erhalten wir:

$$Q_l(x) \geq \frac{2}{27}Q_m(x^{\frac{1}{3}})Q_{m'}(x^{\frac{1}{3}})Q_{m''}(x^{\frac{1}{3}}) + O\left(\frac{1}{\log x}\right) > \frac{1}{20^4(\varphi(k))^3k^3} \text{ für } x > x_0.$$

Daraus folgt Satz 1.2.

5 Quellenangaben

Quellenangaben zu Kapitel 1
Dieses Kapitel basiert auf folgenden Quellen: [5, S.49-51] und [7, S.297].

Quellenangaben zu Kapitel 2

- Definition 2.2: [1, S.24]
- Definition 2.3: [1, S.25]
- Definition 2.4: [1, S.32]
- Definition 2.5: [9, S.9]
- Definition 2.6: [1, S.75]
- Satz 2.7: [1, S.77]
- Satz 2.8: [1, S.82-84]
- Lemma 2.9: [3, S.341-342]
- Satz 2.11: Hier wurden folgende Sätze aus [3] verwendet: Satz 413, Satz 424 und Satz 425.

Quellenangaben zu Kapitel 3

- Definition 3.1: [1, S.133]
- Bemerkung 3.3: [1, S.138]
- Lemma 3.7: [1, Satz 5.12]
- Definition 3.8: [1, S.110]
- Lemma 3.9: [7, S.303]
- Definition 3.10: [6, Definition 5.1.1]
- Definition 3.11: [6, Definition 5.2.1]
- Definition 3.12: [6, Definition 5.3.1]
- Definition 3.13: [4, S.52-53]
- Definition 3.14: [1, S.204]
- Satz 3.15: [2, S.37-38]
- Lemma 3.16: Das Lemma und dessen Beweis folgt [7, S.301-303]. Die Abschätzung der Anzahl Lösungen im 1.Fall bis konkrete Werte für z und y eingesetzt werden stammt von Herrn Pink.

Quellenangaben zu Kapitel 4
Dieses Kapitel folgt [7]. Zusätzlich wurde im Beweis von Lemma 4.1 [8, S.307] verwendet. Des weiteren stammt der Beweis von Lemma 4.4 von Herrn Pink.

Literatur

[1] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, 1976.

[2] Harvey Cohn. *Advanced number theory.* Dover Publications, 1962.

[3] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers.* Oxford University Press, 4 edition, 1975.

[4] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory.* American Mathematical Society, 2004.

[5] Wladyslaw Narkiewicz. *The development of prime number theory - From Euclid to Hardy and Littlewood.* Springer-Verlag, 2000.

[6] Michael Th. Rassias. *Problem-solving and selected topics in number theory.* Springer-Verlag, 2011.

[7] Atle Selberg. An elementary proof of dirichlet's theorem about primes in an arithmetic progression. *Annals of Mathematics*, 50(2):297–304, April 1949.

[8] Atle Selberg. An elementary proof of the prime-number theorem. *Annals of Mathematics*, 50(2):305–313, April 1949.

[9] Jürgen Wolfart. *Einführung in die Zahlentheorie und Algebra.* Vieweg+Teubner, 2 edition, 2011.