8. Vorlesung

Wiederholung.

Für $k \geq 2$, $s \geq 2^k + 1$ gilt

$$R_s(N) = \left(A_s \mathfrak{S}(N) + o(1) \right) N^{\frac{s}{k} - 1},$$

wobei die singuläre Reihe

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} S_N(q)$$

absolut konvergiert. Es gilt

$$S_N(q) = \sum_a{}^{*} \left(\frac{S(q,a)}{q} \right)^s e(-aN/q),$$

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q).$$

Da $S_N(q)$ multiplikativ ist, haben wir das "konvergente" Euler-Produkt

$$\mathfrak{S}(N) = \prod_p T_p(N), \quad T_p(N) = \sum_{m=0}^{\infty} S_N(p^m).$$

Folgerung 8.9. Es gilt $\mathfrak{S}(N) = \prod_p T_p(N)$, wobei

$$T_p(N) = \sum_{n=0}^{\infty} S_N(p^n)$$ absolut konvergiert.

Lemma 8.10. Es gibt eine nur von k, s abhängige Konstante C mit

$$\frac{1}{2} \leq \prod_{p \geq C} |T_p(N)| \leq 2$$

Beweis. Nach Lemma 8.1 gibt's eine Konstante A mit

$$|S_N(q)| \leq \frac{A}{q^{1+2^{-k}}}$$

für alle $q \in \mathbb{N}$. Daher

$$|T_p(N)| \leq 1 + \sum_{n=1}^{\infty} \frac{A}{p^{n(1+2^{-k})}} = 1 + \frac{A}{p^{(1+2^{-k})} - 1}$$

$$\leq 1 + \frac{2A}{p^{1+2^{-k}}} \leq \exp\left(\frac{2A}{p^{1+2^{-k}}}\right).$$

Für beliebiges C ist also

$$\prod_{p\geq C} |T_p(N)| \leq \exp\Big(\sum_{p\geq C} \frac{2A}{p^{1+2^{-k}}} \Big) \leq \exp\Big(\sum_{n\geq C} \frac{2A}{n^{1+2^{-k}}} \Big)$$

Da $\sum_{n=1}^{\infty} \frac{1}{n^{1+2^{-k}}}$ konvergiert ist für hinreichend große C also $\prod_{p\geq C} |T_p(N)| \leq 2$

analog

$$|T_p(N)| \geq 1 - \sum_{n=1}^{\infty} \frac{A}{p^{n(1+2^{-k})}} = 1 - \frac{A}{p^{1+2^{-k}}-1}$$

$$\geq 1 - \frac{2A}{p^{1+2^{-k}}}$$

$$\boxed{1-x \geq e^{-2x} \quad \text{wenn } x \text{ klein}}$$

$$\geq \exp\Big(- \frac{4A}{p^{1+2^{-k}}} \Big)$$

d.h. für große C gilt auch $\prod_{p\geq C} |T_p(N)| \geq \frac{1}{2}$.

Erinnerung In der ersten Vorlesung untersuchten wir

$$M_q(n,s) = |\{(x_1,\dots,x_s) \in (\mathbb{Z}/q\mathbb{Z})^s : x_1^k + \dots + x_s^k = N\}$$

und zeigten

$$\liminf_{t \to \infty} \frac{M_{p^t}(n,s)}{p^{(s-1)t}} > 0 .$$

Genauer zeigten wir sogar

$$\liminf_{t \to \infty} \frac{M_{p^t}(n,s)}{p^{(s-1)t}} \geq p^{-(\tau+2)(s-1)}$$

wobei τ die größte Zahl mit $p^\tau \mid k$ ist.

Satz 8.11. Für alle Primzahlen p und alle $t \in \mathbb{N}$ gilt

$$\sum_{n=0}^{t} S_N(p^n) = \frac{M_{p^t}(N,s)}{p^{(s-1)t}} .$$

Beweis. Wir betrachten

$$\Omega = \sum_{a=1}^{p^t} \Big(\sum_{r=1}^{p^t} e(ar^k \mid p^t) \Big)^s e(-aN \mid p^t).$$

Einerseits ist

$$\Omega = \sum_{a=1}^{p^t} \sum_{r_1=1}^{p^t} \sum_{r_2=1}^{p^t} \cdots \sum_{r_s=1}^{p^t} e(a(r_1^k + \ldots + r_s^k - N)/p^t)$$

$$= \sum_{r_1} \cdots \sum_{r_s} \begin{cases} p^t & \text{wenn } r_1^k + \ldots + r_s^k \equiv N \pmod{p^t} \\ 0 & \text{sonst} \end{cases}$$

$$= p^t M_{p^t}(N, s).$$

Andererseits kann man jedes $a \in [p^t]$ in der Form $a = p^{t-n} \cdot a'$ mit $0 \leq n \leq t$, $ggT(p, a') = 1$, $1 \leq a' \leq p^n$ schreiben.

Also

$$\Omega = \sum_{n=0}^{t} \sum_{a'=1}^{p^n}{}^{*} \Big(\sum_{r=1}^{p^t} e(a' r^k \mid p^n) \Big)^s e(-a' N \mid p^n).$$

In der inneren Summe werden die Reste modulo p^n je p^{t-n} mal durchlaufen. Daher

$$\Omega = \sum_{n=0}^{t} \sum_{a'=1}^{p^n}{}^{*} \Big(p^{t-n} \cdot \underbrace{\sum_{r=1}^{p^n} e(a' r^k \mid p^n)}_{= S(p^n, a')} \Big)^s e(-a' N \mid p^n)$$

$$= \sum_{n=0}^{t} \sum_{a'=1}^{p^n}{}^{*} \Big(p^t \, \frac{S(p^n, a')}{p^n} \Big)^s e(-a' N \mid p^n)$$

$$= p^{st} \sum_{n=0}^{t} S_{p^n}(N)$$

Somit ist in der Tat

$$\sum_{n=0}^{t} S_{p^n}(N) = \frac{\Omega}{p^{st}} = \frac{M_{p^t}(N, s)}{p^{(s-1)t}} . \qquad \square$$

Folgerung 8.12 Für jede Primzahl p ist

$$|T_p(N)| \geq p^{-(\tau+2)(s-1)}$$

wobei τ die größte Zahl mit $p^\tau \mid k$ ist.

Folgerung 8.13. Es gibt eine nur von $k \geq 2$ und $s \geq 2^k+1$ abhängige Konstante $\gamma > 0$ mit $\mathfrak{S}(N) \geq \gamma$ für alle $N \in \mathbb{N}$.

Beweis. Wir wissen $\mathfrak{S}(N) = \prod_p T_p(N)$.

Nach Lemma 8.10 gibt's $C > 0$ mit $\prod_{p > C} |T_p(N)| \geq \frac{1}{2}$ für alle $N \in \mathbb{N}$. Für jede Primzahl $p < C$ gibt's nach Folgerung 8.12 ein $\gamma_p > 0$ mit $|T_p(N)| \geq \gamma_p$.

Nun tut's $\gamma = \frac{1}{2} \prod_{p < C} \gamma_p$. $\square$

Satz 8.14. Für $k \geq 2$ und $s \geq 2^k + 1$ ist jede hinreichend große Zahl N als Summe von s k^{ten} Potenzen darstellbar. Die Anzahl der Darstellungen ist $\Omega(N^{\frac{s}{k} - 1})$.

Beweis. Benutze die Folgerungen 8.3 und 8.13. $\square$

§9. Eine weitere Anwendung der Weyl'schen Ungleichung.

Satz 9.1. Es gibt ein $t_0 \in \mathbb{N}$ mit folgender Eigenschaft:

Für alle ganzen Zahlen $t \geq t_0$, $N > t$ und alle $a \in \mathbb{Z}$ gibt's $p \in [t]$ mit

$$\left\| \frac{ap^2}{N} \right\| \leq t^{-1/6}.$$

Erinnerung Für jede Funktion $f : (\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}$ ist die Fouriertransformierte $\hat{f} : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}$ durch

$$\hat{f}(r) = \sum_{n=0}^{N-1} f(n) \cdot e(-rn/N)$$

definiert. Es gilt dann die Formel von Parseval

$$\sum_{n=0}^{N-1} |f(n)|^2 = \frac{1}{N} \sum_{r=0}^{N-1} |\hat{f}(r)|^2.$$

[Warum? $\displaystyle\sum_{r=0}^{N-1} |\hat{f}(r)|^2 = \sum_{r=0}^{N-1} \sum_{n=0}^{N-1} f(n) e(-rn/N) \sum_{n'=0}^{N-1} \overline{f(n')} e(rn'/N)$

$$= \sum_{n=0}^{N-1} \sum_{n'=0}^{N-1} f(n)\, \overline{f^*(n')} \underbrace{\sum_{r=0}^{N-1} e((n'-n)r/N)}_{= \begin{cases} N & \text{wenn } n=n' \\ 0 & \text{wenn } n\neq n' \end{cases}}$$

$$= N \sum_{n=0}^{N-1} |f(n)|^2 \qquad]$$

Die <u>Faltung</u> von $f, g : (\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}$

ist die Funktion $f * g : (\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}$

mit $$(f*g)(x) = \sum_{y+z=x} f(y)\, g(z).$$

Wir identifizieren oft Teilmengen $A \subseteq \mathbb{Z}/N\mathbb{Z}$ mit ihren charakt. Fkt. (d.h. $A(x) = 0$ wenn $x \notin A$, $A(x) = 1$ wenn $x \in A$) und ganze Zahlen mit ihren Restklassen modulo N.

Das Intervall $[-M, M) \subseteq \mathbb{Z}/N\mathbb{Z}$ ist also die Menge

$$\{-M + N\mathbb{Z}, \ldots, (M-1) + N\mathbb{Z}\}.$$

<u>Lemma 9.2.</u> Es seien M, N natürliche Zahlen mit $N > 2M$ und $I = [-M, M) \subseteq \mathbb{Z}/N\mathbb{Z}$. Für alle $r \in \mathbb{Z}$ ist

$$|\hat{I}(r)| \leq \min\left(2M, \frac{1}{2\|r/N\|}\right).$$

<u>Beweis.</u> Es ist

$$\hat{I}(r) = \sum_{n=-M}^{M-1} e(-nr/N)$$

Aus der Δ-Ungl. folgt also $|\hat{I}(r)| \leq 2M$.

Ferner

$$|\hat{I}(r)| = \left|\frac{e(Mr/N) - e(-Mr/N)}{1 - e(r/N)}\right| \leq \frac{2}{|1 - e(r/N)|}.$$

Da
$$|1-e(\tfrac{r}{N})| = 2|\sin \tfrac{\pi r}{N}| \geq 4\|\tfrac{r}{N}\|$$
folgt
$$|\hat{I}(r)| \leq \frac{1}{2\|\frac{r}{N}\|}. \qquad \square$$

<u>Lemma 9.3.</u> Es seien $M \in \mathbb{N}$ gerade, $N > 2M$ und $f : \mathbb{Z}/N\mathbb{Z} \longrightarrow [0,\infty)$ eine Funktion mit $\mathrm{supp}(f) \cap [-M, M) = \emptyset$. Dann gibt's $r \in \mathbb{Z}$ mit $N \nmid r$,
$$\|\tfrac{r}{N}\| \leq \frac{N}{M^2} \quad \text{und} \quad |\hat{f}(r)| \geq \frac{\hat{f}(0)\,M}{2N}.$$

<u>Beweis.</u> Setze $J = [-\frac{M}{2}, \frac{M}{2})$. Wegen $(J-J) \cap \mathrm{supp}(f) = \emptyset$ ist
$$\sum_{r=0}^{N-1} \hat{f}(r)\,|\hat{J}(r)|^2 = \sum_{r=0}^{N-1} \sum_{a \in \mathrm{supp}(f)} f(a)\, e(-ar/N).$$

$$\cdot \sum_{j \in J} e(-aj r/N) \sum_{j' \in J} e(aj' r/N)$$

$$= \sum_{a \in \mathrm{supp}(f)} \sum_{j \in J} \sum_{j' \in J} f(a) \sum_{r=0}^{N-1} e\Big(\underbrace{(-a-j+j')}_{\text{nicht durch } N \text{ teilbar}} r/N \Big)$$

$$= 0 .$$