3. Vorlesung.

Wiederholung

Sei $k \geq 2$ fest.

Ziel: Jede hinr. große nat. Zahl ist Summe von 2^k+1 k^{ten} Potenzen.

Satz 2.10. Für alle $s \geq 2^k+1$ und alle Primzahlen p gilt

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

wobei $M_{p^t}(n,s) = |\{(x_1,\dots,x_s) \in (\mathbb{Z}/p^t\mathbb{Z})^s : x_1^k + \dots + x_s^k = n\}|$.

Setze $J_s(n) = \sum_{m_1+\dots+m_s=n} \frac{1}{k^s}(m_1 \cdot \ldots \cdot m_s)^{\frac{1}{k}-1}$.

Dann $J_s(n) = A_s n^{\frac{s}{k}-1} + O(n^{\frac{s-1}{k}-1})$, wobei $A_s > 0$ von n unabhängige Konstante.

Außerdem $J_s(n) = \int_{-1/2}^{+1/2} v(\beta)^s e(-n\beta)\,d\beta$, wobei

$$v(\beta) = \sum_{m=1}^{n} \frac{1}{k} m^{1-\frac{1}{k}} e(m\beta).$$

$$\boxed{e(\alpha) = e^{2\pi i\alpha}}$$

Es gilt $|v(\beta)| \leq n^{1/k}$ und $|v(\beta)| \leq 2|\beta|^{-1/k}$ für $|\beta| \leq \frac{1}{2}$, $\beta \neq 0$.

Folgerung 3.5. Sei $s > k$. Für jede Folge $(\delta_n)_{n\in\mathbb{N}}$ positiver reeller Zahlen mit $n\delta_n \longrightarrow \infty$ ist

$$\left| J_s(n) - \int_{-\delta_n}^{+\delta_n} \nu(\beta)^s \, e(-n\beta)\, d\beta \right| = o\left(n^{\frac{s}{k}-1}\right).$$

Beweis. Die linke Seite ist

$$\leq 2 \left| \int_{\delta_n}^{1/2} \nu(\beta)^s \, e(-n\beta)\, d\beta \right| \leq 2 \int_{\delta_n}^{1/2} |\nu(\beta)|^s \, d\beta$$

$$\leq 2^{s+1} \int_{\delta_n}^{1/2} |\beta|^{-s/k} \, d\beta = 2^{s+1} \left. \frac{\beta^{1-\frac{s}{k}}}{1-\frac{s}{k}} \right]_{\delta_n}^{1/2}$$

$$\leq 2^{s+1} \frac{\delta_n^{1-\frac{s}{k}}}{\frac{s}{k}-1} = O\left(\left(\frac{1}{\delta_n}\right)^{\frac{s}{k}-1}\right) = o\left(n^{\frac{s}{k}-1}\right). \quad \square$$

§4. Asymptotische Formeln.

Wir suchen eine asymptotische Formel für

$$R_s(n) = |\{(x_1, \ldots, x_s) \in \mathbb{N}^k : x_1^k + \ldots + x_s^k = n\}|$$

Wie sehr soll man $R_s(n) \approx J_s(n)$ glauben?

Für $k=4$ ist $R_{14}(16t+15) = 0$ für alle $t \in \mathbb{N}$, aber

$J_{14}(n) = A n^{5/2} + O(n^{9/4})$ für eine geeignete Konstante $A > 0$.

Eine bessere Näherung könnte die Form

$$R_s(n) \approx \prod_{p \text{ prim}} T_p(n) \cdot J_s(n)$$

haben, wobei

$$T_p(n) = \lim_{t \to \infty} \frac{M_{p^t}(n,s)}{p^{(s-1)t}}.$$

Wir zeigen, dass für $s \geq 2^{k+1}$ dieser Limes existiert,

$$\mathfrak{S}(n) = \prod_{p \text{ prim}} T_p(n)$$

konvergiert und $\mathfrak{S}(n) = \Omega(1)$.

. . . . . .

Primzahlzwillinge. Für $x > 0$ setze

$$\pi(x) = |\{p \leq x : p \text{ prim}\}|.$$

Der Primzahlsatz sagt

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

Manchmal verhält sich die Menge der Primzahlen wie eine zufällige Menge $Z \subseteq \mathbb{N}$ mit

$$\mathbb{P}(m \in Z) = \frac{1}{\log m} \quad \text{für } m \geq 3$$

Setze
$$\pi_2(x) = |\{ p \le x : p, p+2 \text{ sind prim} \}|.$$

Alle glauben $\pi_2(x) \longrightarrow \infty$ für $x \longrightarrow \infty$.

Wie könnte eine asymptotische Formel für $\pi_2(x)$ aussehen?

Betrachte
$$J(x) = \sum_{3 \le m \le x} \frac{1}{\log m} \frac{1}{\log(m+2)}$$
$$= \mathbb{E}\, |\{ m \le x : m, m+2 \in Z \}| .$$

Man kann $J(x) \sim \dfrac{x}{(\log x)^2}$ zeigen.

Empirisch unterscheiden sich $\pi_2(x)$, $J(x)$ um den Faktor 1,3203 ---- Betrachte Korrekturfaktoren
$$C_p = \frac{\mathbb{P}(p \nmid m+2 : p \nmid m)}{\mathbb{P}(p \nmid m+2)} .$$

Genauer $\quad C_2 = \frac{1}{1/2} = 2$

$$C_p = \frac{(p-2)/(p-1)}{(p-1)/p} = \frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2} \quad \text{für ungerade } p.$$

Satz $\quad C = \prod_{p \text{ prim}} C_p = 1{,}3203\ldots$

Diese Zahl heißt Zwillingskonstante.

<u>Vermutung</u> $\quad \pi_2(x) \sim \frac{Cx}{(\log x)^2}$

<u>Satz (Selberg)</u> $\quad \pi_2(x) \leq (2 + o(1)) \cdot \frac{Cx}{(\log x)^2}.$

$\mathbb{R} \qquad \mathbb{Q}_p$

§5. Die Weyl'sche Ungleichung.

Gäbe es $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ mit

$$\{\alpha \cdot n^3\} = 0.2473\ldots$$

für fast alle $n \in \mathbb{N}$, dann

$$\{\alpha(n_1^3 + \ldots + n_9^3)\} = \{9 \cdot 0{,}2473\ldots\}$$

$$= 0{,}025\ldots$$

und es könnte nicht $G(3) \leq 9$ sein.

In dieser Situation wäre $\left|\sum_{m=1}^{n} e(\alpha m^3)\right| \approx n$.

Wir untersuchen daher

$$\left|\sum_{m=1}^{n} e(P(m))\right|,$$ wobei P ein Polynom ist.

<u>Spezialfall 1:</u> $P = \alpha x + \beta$, wobei $\alpha, \beta \in \mathbb{R}$.

Dann $\left| \sum_{m=1}^{n} e(P(m)) \right| = \left| \sum_{m=1}^{n} e(\alpha m) \right|$.

Wir wissen bereits

$$\left| \sum_{m=1}^{n} e(\alpha m) \right| \leq \frac{1}{2|\alpha|} \quad \text{wenn} \quad |\alpha| \leq \tfrac{1}{2},\ \alpha \neq 0.$$

Setzt man

$$\|\alpha\| = \min \{ |\alpha - z| : z \in \mathbb{Z} \}$$

so ist also

$$\left| \sum_{m=1}^{n} e(P(m)) \right| \leq \min\left(n, \frac{1}{2\|\alpha\|}\right).$$

<u>Spezialfall 2:</u> $P(x) = \alpha x^2 + \beta x + \gamma$, wobei $\alpha, \beta, \gamma \in \mathbb{R}$.

Setze $S = \sum_{m=1}^{n} e(P(m))$.

Nun $|S|^2 = \sum_{m=1}^{n} \sum_{m'=1}^{n} e(P(m') - P(m))$

$$\leq n + 2 \Big| \sum_{1 \leq m < m' \leq n} e(P(m') - P(m)) \Big|$$

$m' = m + h$

$$\leq n + 2 \sum_{h=1}^{n-1} \Big| \sum_{m=1}^{n-h} e(P(m+h) - P(m)) \Big|$$

Da

$$P(m+h) - P(m) = \alpha (m+h)^2 + \beta (m+h) + \gamma$$
$$- \alpha m^2 - \beta m - \gamma$$
$$= \alpha (2mh + h^2) + \beta h$$
$$= 2\alpha h \cdot m + (\alpha h^2 + \beta h)$$

folgt

$$|S|^2 \leq n + 2 \sum_{h=1}^{n-1} \Big| \sum_{m=1}^{n-h} e(2\alpha h \cdot m) \Big|$$

$$\leq n + 2 \sum_{h=1}^{n-1} \min\Big(n, \frac{1}{2\|2\alpha h\|} \Big)$$

$$\leq n + \sum_{h=1}^{2n} \min\Big(2n, \frac{1}{\|\alpha h\|} \Big).$$

Dies führt uns auf das Problem, Summen der Form

$$\sum_{h=1}^{H} \min\left(n, \frac{1}{\|\alpha h\|}\right)$$

abzuschätzen.

. . . . . .

Lemma 5.1. (Dirichlet) Es seien $\alpha \in \mathbb{R}$ und $Q \in \mathbb{N}$.

Dann gibt's $a \in \mathbb{Z}$ und $q \in [Q]$ mit $\mathrm{ggT}(a, q) = 1$

und
$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q(Q+1)} < \frac{1}{q^2}.$$

Beweis. Angenommen, es gäbe kein $q \in [Q]$ mit $\{\alpha q\} \in [0, \frac{1}{Q+1}) \cup [\frac{Q}{Q+1}, 1)$.

Dann wären die Q Zahlen $\{\alpha\}, \{2\alpha\}, \ldots, \{Q\alpha\}$

in den $Q-1$ Schubfächern $[\frac{1}{Q+1}, \frac{2}{Q+1}), \ldots [\frac{Q-1}{Q+1}, \frac{Q}{Q+1})$.

Nach Schubfachprinzip gäbe es dann $1 \le r_1 < r_2 \le Q$ und j mit $\{r_1\alpha\}, \{r_2\alpha\} \in \left[\frac{j}{Q+1}, \frac{j+1}{Q+1}\right)$.

Doch dann

$$\{(r_2-r_1)\alpha\} \in \begin{cases} \left[0, \frac{1}{Q+1}\right) & \text{wenn } \{r_1\alpha\} \le \{r_2\alpha\} \\ \left[\frac{Q}{Q+1}, 1\right) & \text{wenn } \{r_1\alpha\} > \{r_2\alpha\} \end{cases}$$

Wähle nun $q \in [Q]$ mit

$$\{q\alpha\} \in \left[0, \frac{1}{Q+1}\right) \cup \left[\frac{Q}{Q+1}, 1\right),$$

und dann $a \in \mathbb{Z}$ mit

$$|q\alpha - a| \le \frac{1}{Q+1}.$$

Division durch q ergibt $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q(Q+1)}$.

Wenn $\mathrm{ggT}(a,q) > 1$ kann man kürzen. $\square$

<u>Lemma 5.2.</u> Wenn $\alpha = \frac{a}{q}$, wobei $a \in \mathbb{Z}$, $q \in \mathbb{N}$, $ggT(a, q) = 1$, dann gilt

$$\sum_{h=m}^{m+q-1} \min\left(n, \frac{1}{\|\alpha h\|}\right) \leq n + 2q \log 2q$$

für alle $m, n \in \mathbb{N}$.

<u>Beweis.</u> Die Zahlen $\{\alpha m\}, \ldots, \{\alpha(m+q-1)\}$ stimmen mit $0, \frac{1}{q}, \frac{2}{q}, \ldots, \frac{q-1}{q}$ überein. Daher

$$\sum_{h=m}^{m+q-1} \min\left(n, \frac{1}{\|\alpha h\|}\right) \leq n + 2 \sum_{j \leq q/2} \frac{1}{j/q}.$$

Es genügt also

$$\sum_{j \leq q/2} \frac{1}{j} \leq \log(2q) \quad \text{-------} \quad (5.1)$$

zu zeigen. Für $q = 1$ ist das klar. Für $q \geq 2$ ist

$$\sum_{j \leq q/2} \frac{1}{j} \leq 1 + \int_1^{q/2} \frac{dt}{t} = 1 + \log \frac{q}{2} \leq \log 2q. \quad \square$$