Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a1: Einführung, Riemannsche Zetafunktion

Stichworte: Analytische ZT, Eigenschaften der Riemannschen Zetafunktion: Reihen- und Produktdarstellung für $\sigma > 1$, kritischer Streifen, meromorphe Fortsetzung auf $\mathbb{C}$

1.1. Einleitung: Die Vorlesung "Zahlentheorie II" behandelt klassische Sätze und Methoden der analytischen Zahlentheorie. Wir verweisen auf die Ergebnisse, die in der früheren BSc-Vorlesung Analytische Zahlentheorie "AnZ" behandelt wurden. Diese frühere Vorlesung wird nicht unmittelbar vorausgesetzt, deren Besuch kann aber vorteilhaft zum Verständnis der Vorlesungsinhalte sein. Dort angesprochene Themen werden in dieser Vorlesung vertieft, ergänzt, und teilweise durch Nennung von sehr neuen Forschungsergebnissen auf den aktuellen Stand gebracht.

Zum Unterschied zur BSc-Vorlesung zeigen wir im ersten Teil der Vorlesung den PZS mit Restglied bzw. das Vinogradov-Korobov-nullstellenfreie Gebiet für ζ. Der direkte Zusammenhang wird mit der expliziten Formel für ψ deutlich. Es kommt die Perronsche Formel zum Einsatz, wir zeigen Sätze zur Nullstellenanzahl in Abschnitten des kritischen Streifens. Neueste Ergebnisse über Weylsche Exponentialsummen im Zusammenhang mit Vinogradovs Mittelwertsatz werden außerdem verwendet.
Im zweiten Teil der Vorlesung untersuchen wir Dirichletsche L-Reihen im Hinblick auf die Theorie der Primzahlverteilung in arithmetischen Progressionen. Wir behandeln über den PZS in APs hinaus die Problematik der Gleichmäßigkeit der Ergebnisse im Modul q. Dies führt uns u.a. auf den Satz von Siegel, von Siegel-Walfisz, von Bombieri-Vinogradov und Brun-Titchmarsh. Dabei werden wir Siebmethoden einsetzen, insbesondere das sogenannte große Sieb. Danach kommen noch Dedekindsche Zetafunktionen und die Klassenzahlformel für quadratische Zahlkörper zur Sprache, und zu guter letzt die Kreismethode und das Goldbachsche Problem.

Wir beginnen mit der Riemannschen ζ-Funktion und ihren grundlegenden Eigenschaften. Diese wurden in Anz(10) bereits gezeigt.

1.2. Konvention: $s = \sigma + it \in \mathbb{C}$, d.h. $\operatorname{Re} s = \sigma$, $\operatorname{Im} s = t$.

1.3. Def.: Die Riemannsche Zetafunktion $\zeta(s)$ ist für $\sigma > 1$ durch die Dirichletreihe $\zeta(s) = \sum_{n \geq 1} n^{-s}$ definiert (die dort Kgt., in $s=1$ nicht mehr).

1.4. Satz: Für $\sigma > 1$ ist $\zeta(s)$ holomorph und hat dort die Eulerproduktdarstellung

Euler-Produkte: vgl. Anz 8

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}.$$

Insb. ist dort $\zeta(s) \neq 0$ und $\frac{1}{\zeta(s)} = \sum_{n \geq 1} \mu(n) n^{-s}$.

Dabei ist $\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^r, & n = p_1 \cdots p_r \\ 0, & \text{sonst} \end{cases}$ die Möbius-Fkt.

Bem.: Die Reihe $\sum_{n \geq 1} n^{-s}$ divergiert in jedem $s = 1 + it$, $t \in \mathbb{R}$, laut Anz 10.9.

1.5. Satz: Die Fkt. $\zeta(s)$ lässt sich meromorph fortsetzen auf den Bereich $\sigma > 0$ mit der Formel

$$\zeta(s) = \frac{1}{(s-1)^1} - s \int_1^\infty \frac{u - \lfloor u \rfloor - \frac{1}{2}}{u^{s+1}} \, du + \frac{1}{2}.$$

Daran ablesbar: Einzige Singularität ist Pol 1-ter Ordnung bei $s = 1$ vom Residuum 1.

vgl. Anz 10.5 → Bew.: Anw. der Eulerschen Summenformel 1.6. für $\sigma > 1$, $\varepsilon > 0$ bel. klein, zeigt

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \int_{1-\varepsilon}^\infty u^{-s} \, du - s \int_{1-\varepsilon}^\infty P_0(u) u^{-s-1} \, du + (1-\varepsilon)^{-s} P_0(1-\varepsilon)$$

$$\overset{\varepsilon \to 0}{=} \int_1^\infty u^{-s} \, du - s \int_1^\infty P_0(u) u^{-s-1} \, du + \frac{1}{2} = \frac{1}{s-1} - s \int_1^\infty \frac{u - \lfloor u \rfloor - \frac{1}{2}}{u^{s+1}} \, du + \frac{1}{2}.$$

Da $|u - \lfloor u \rfloor - \frac{1}{2}| \leq \frac{1}{2}$, ist $\int_1^\infty \frac{u - \lfloor u \rfloor - \frac{1}{2}}{u^{s+1}} \, du$ kompakt kgt. in $\sigma > 0$.

Daher stellt $s \int_1^\infty \frac{u - \lfloor u \rfloor - \frac{1}{2}}{u^{s+1}} \, du$ eine in $\sigma > 0$ holomorphe Fkt. dar. □

1.6. Eulersche Summenformel:

Seien $c < x$ reell, sei $f : [c, x] \to \mathbb{C}$ stetig und stückweise stetig diff'bar auf $[c, x]$.

Setze $P_0(x) := x - \lfloor x \rfloor - \frac{1}{2}$ (diese "Sägezahnkurve" wird gelegentlich auch mit $\psi(x)$ bezeichnet; hier nicht, weil ψ schon für die 2. Tsch.-Funktion reserviert ist.)

Dann ist

$$\sum_{c < n \leq x} f(n) = \int_c^x f(u) \, du + \int_c^x P_0(u) f'(u) \, du - f(x) P_0(x) + f(c) P_0(c).$$

Bew.: Vgl. Anz 3.24, ist Nachrechnen. □

Bem.: Die Formel gilt genauso mit $\{u\} := u - \lfloor u \rfloor$ anstelle $P_0(u)$; klar.

1.7. **Def.:** Der so gewonnene Fortsetzungsbereich $0 < \sigma \leq 1$ heißt Kritischer Streifen der Zetafunktion.

1.8. **Bem.:** Die Aussage $\zeta(s) \neq 0$ für $\sigma = 1$, bewiesen von de la Valée-Poussin/Hadamard führt zum Beweis des PZSes $\pi(x) \sim \frac{x}{\lg x}$, wo $\pi(x) := \#\{p \leq x\}$.
Dies werde in Anz 13 – Anz 16 gezeigt. Ziel dieser Vorlesung: Weitere Kenntnis über nullstellenfreie Gebiete im kritischen Streifen verbessert den PZS-Fehlerterm!

Die Funktion ζ lässt sich nach $\sigma \leq 0$ weiter meromorph fortsetzen wie folgt:

1.9. **Satz** (Funktionalglg. der Riemannschen Zetafunktion):
Die Fkt. ζ besitzt eine merom. Forts. in $\mathbb{C}$ mit einem einzigen Pol bei $s = 1$ der Ordnung 1 vom Residuum 1. Die vollständige Zetafunktion $\xi(s) := \Gamma(\frac{s}{2}) \pi^{-s/2} \zeta(s)$ erfüllt die Funktionalglg. $\xi(s) = \xi(1-s)$, $s \in \mathbb{C} \setminus \{0,1\}$. Dabei ist $\xi(s) \neq 0$ für $\sigma < 0$ und $\sigma > 1$.

Bew.: In Anz 18 – Anz 20.
Also: ξ hol. auf $\mathbb{C} \setminus \{0,1\}$. Mit $\xi(s) \neq 0$ für $\sigma > 1$ folgt $\xi(s) \neq 0$ für $\sigma < 0$. $\square$

1.10. **Kor.:** Die Fkt. ζ hat keine Nst. in $\sigma > 1$, und in $\sigma < 0$ genau die (trivialen) Nst. $-2, -4, -6, \ldots$ (welche die Γ-Pole dort aufheben).
Für die (nichttrivialen) Nst. im kritischen Streifen $0 \leq \sigma \leq 1$ gilt: $\zeta(s) = 0 \Leftrightarrow \zeta(1-s) = 0$.

1.11. **Bem.:** $\zeta(s) = 0 \Leftrightarrow \overline{\zeta(s)} = 0 \Leftrightarrow \zeta(\bar{s}) = 0$ im kritischen Streifen.
Diese Symmetrie zeigt, dass jede nichttriv. Nst. $\varrho = \beta + i\gamma$ mit $\beta \neq \frac{1}{2}$, $\gamma \neq 0$, gleich ein Quadrupel $\varrho, \bar{\varrho}, 1-\varrho, 1-\bar{\varrho}$ von Nullstellen impliziert.

1.12. **Zusatz:** Die Funktionalgleichung erlaubt es nicht unmittelbar, $\zeta(0)$ zu bestimmen.
Eine Berechnung ist etwa so möglich:

$$\zeta(0) = \underbrace{\pi^{-1/2}\,\Gamma(\tfrac{1}{2})}_{=1} \lim_{s \to 0} \frac{\zeta(1-s)}{\Gamma(s/2)} = \lim_{s \to 0} \frac{\frac{1}{(1-s)-1} + H(s)}{\Gamma(1+s/2)/s/2} = \lim_{s \to 0} \frac{s}{2}\left(\frac{-1/s}{\Gamma(1+s/2)} + \ldots\right) = -\frac{1}{2}.$$

Die Fortsetzungsformel aus 1.5 erlaubt es, ζ auf der positiven reellen Achse abzuschätzen:

1.13. **Satz:** Für alle $\sigma>0$ gilt $\frac{1}{\sigma-1} < \zeta(\sigma) < \frac{\sigma}{\sigma-1} = 1+\frac{1}{\sigma-1}$.

Speziell für $0<\sigma<1$ gilt damit $\zeta(\sigma)<0$; also hat ζ dort keine Nullstellen.

Bew.: Durch $\{u\} := u - \lfloor u \rfloor$ bringen wir 1.5 (für $\sigma>0$) zunächst auf die Form

$$\zeta(s) = \frac{1}{s-1} - s\int_1^\infty \frac{u-\lfloor u\rfloor-\frac12}{u^{s+1}}\,du + \frac12 = \frac{1}{s-1} + \frac12 + \frac12 s \underbrace{\int_1^\infty \frac{du}{u^{s+1}}}_{=\frac{-1}{s}u^{-s}\big|_1^\infty = \frac{1}{s}} - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du$$

$$= 1 + \frac{1}{s-1} - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du,$$

mit der Ungleichung $0\le\{u\}<1$ folgt $0 \le \int_1^\infty \frac{\{u\}}{u^{\sigma+1}}\,du < \int_1^\infty u^{-\sigma-1}\,du = \frac{1}{\sigma}$ für $\sigma>0$.

Somit ist $\zeta(\sigma) > 1+\frac{1}{\sigma-1} - \sigma\cdot\frac{1}{\sigma} = \frac{1}{\sigma-1}$ und $\zeta(\sigma) < 1+\frac{1}{\sigma-1}$. $\square$

Aus der Dirichletreihen- und Eulerproduktdarstellung von ζ in $\sigma>1$ folgt noch:

1.14. **Satz:** Für $\sigma>1$ gilt $\log\zeta(s) = \sum_{n\ge1} \frac{\Lambda(n)}{\log(n)} n^{-s}$ und $\underbrace{-\frac{\zeta'(s)}{\zeta(s)}}_{\text{logarithmische Ableitung von } \zeta} = \sum_{n\ge1} \Lambda(n) n^{-s}$

Vgl. Ü

Dabei ist $\Lambda(n) = \begin{cases} \log(p), & n=p^k \text{ für ein } p\in\mathbb{P},\ k\ge1, \\ 0, & \text{sonst} \end{cases}$ die von-Mangoldt-Funktion.

Die folgende Abschätzung von ζ wird oft benutzt:

1.15. **Satz:** Sei $\delta>0$. Dann ist $\zeta(s) = \frac{1}{s-1} + O(1)$ gleichmäßig im Rechteck $\delta\le\sigma\le2$, $|t|\le1$, und in $\delta\le\sigma\le2$, $|t|\ge1$, gilt gleichmäßig die Abschätzung

$$\zeta(s) \ll (1+\tau^{1-\sigma})\min\left(\frac{1}{|\sigma-1|}, \log(\tau)\right), \quad \text{wo } \tau := |t|+4.$$

Bew.: • Wegen $\zeta(s) = 1+\frac{1}{s-1} - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du$ ist die erste Beh. klar,

denn $\int_1^x u^{-s-1}\,du = \frac{-1}{s}u^{-s}\big|_1^x = \frac1s - \frac{x^{-s}}{s}$, und $\left|\frac{x^{-s}}{s}\right| \le \frac1\delta\cdot x^{-\sigma} \le \frac{x^{-\delta}}{\delta} \xrightarrow[x\to\infty]{} 0$.

• Sei $x\ge2$. Glm. in $\sigma\ge0$ ist $\sum_{n\ge1} n^{-s} \ll \sum_{n\ge1} n^{-\sigma} \ll 1+\int_1^x u^{-\sigma}\,du$.

* Falls $0\le\sigma\le 1-\frac{1}{\log(x)}$, ist $\int_1^x u^{-\sigma}\,du = \frac{x^{1-\sigma}-1}{1-\sigma} < \frac{x^{1-\sigma}}{1-\sigma}$.

* Falls $|\sigma-1|\le\frac{1}{\log(x)}$, ist $u^{-\sigma} \asymp u^{-1}$ glm. in $1\le u\le x$, also $\int_1^x u^{-\sigma}\,du \asymp \int_1^x u^{-1}\,du = \log(x)$.

$\left(\sigma\log(u) = \log(u) + \frac{\log(u)}{\log(x)}\right)$

* Falls $\sigma\ge 1-\frac{1}{\log(x)}$, ist $\int_1^x u^{-\sigma}\,du < \frac{1}{\sigma-1}$.

Insg. ist $\sum_{n\le x} n^{-s} \ll (1+x^{1-\sigma})\min\left(\frac{1}{|\sigma-1|}, \log(x)\right)$, glm. in $0\le\sigma\le2$. Wähle nun $x=\tau$ in der Formel aus 1.16, damit folgt die Beh., denn $\int_x^\infty \{u\}u^{-s-1}\,du \ll \int_x^\infty u^{-\sigma-1}\,du = \frac{x^{-\sigma}}{\sigma}$. $\square$

1.16. <u>Satz:</u> Für $\sigma>0$, $x>0$, $s\neq 1$ gilt

$$\zeta(s) = \sum_{n\leq x} n^{-s} + \frac{x^{1-s}}{s-1} + \frac{\{x\}}{x^s} - s\int_x^\infty \{u\}u^{-s-1}\,du.$$

<u>Bew.:</u> Für $\sigma>1$ gilt

Eulersche Σ-Formel 1.6, $f(u)=u^{-s}$, $\{u\}$ statt $P_0(u)$

$$\sum_{1\leq n\leq x} n^{-s} = \zeta(s) - \sum_{n>x} n^{-s} = \zeta(s) - \underbrace{\int_x^\infty u^{-s}\,du}_{=\frac{u^{-s+1}}{1-s}\Big|_x^\infty = -\frac{x^{1-s}}{1-s}} + s\int_x^\infty \{u\}u^{-s-1}\,du - \{x\}x^{-s},$$

fertig.

(–, da x die u. Gr. des $\int$) $\square$

1.17. <u>Bem.:</u> Diese Formel bietet die Möglichkeit, ζ mit Partialsummen der Dirichletreihe abzuschätzen, selbst, wenn die Reihe (in $0<\sigma\leq 1$) divergiert, außer für $s=1$.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a2: Primzahlzählfunktionen und PZS

Stichworte: Primzahlzählfunktionen π, ϑ, ψ, Satz von Tschebyschev, Primzahlsatz, Riemannsche Vermutung, Zusammenhang zwischen ζ und Λ bzw. ψ

2.1. Einleitung: Wir behandeln die drei gängigen Primzahlzählfunktionen π, ϑ, ψ (und kurz ihre Verallgemeinerungen auf eine arithmetische Progression $a \bmod q$).

2.2. Def.: Sei $x>1$ reell. Def. $\pi(x) := \#\{p \le x;\ p \in \mathbb{P}\} = \sum_{p \le x} 1$.
Seien $q, a \in \mathbb{Z}$, $q \ge 1$. Def. $\pi(x; q, a) := \#\{p \le x;\ p \in \mathbb{P},\ p \equiv a\ (q)\}$
$$= \sum_{\substack{p \le x \\ p \equiv a\ (q)}} 1.$$

Mit "Primzahlzählfunktion" ist meist $\pi(x)$ bzw. $\pi(x; q, a)$ gemeint. Es gibt noch die folgenden (gewichteten) Varianten, die technisch leichter handzuhaben sind:

2.3. Def.: Sei $x>1$ reell. Def. $\vartheta(x) := \sum_{p \le x} \log(p)$
Seien $q, a \in \mathbb{Z}$, $q \ge 1$. Def. $\vartheta(x; q, a) := \sum_{\substack{p \le x \\ p \equiv a\ (q)}} \log(p)$.

2.4. Def.: Die von-Mangoldt-Funktion Λ ist def. als
$\Lambda(n) = \log(p)$, falls n eine Primpotenz (zu einer PZ p) ist, d.h.
$$\exists\, p \in \mathbb{P}\ \exists\, k \in \mathbb{N} : n = p^k,$$
und $\Lambda(n) = 0$, sonst.

2.5. Bem.: Haben $\sum_{d \mid n} \Lambda(d) = \log(n)$, da für $n \overset{\text{PFZ}}{=} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ gilt: l.S. $= \sum_{i=1}^{r} \sum_{\beta_i \le \alpha_i} \log(p_i) = \sum_{i=1}^{r} \log(p_i^{\alpha_i}) = \log(n)$.

2.6. Def.: Sei $x>1$ reell. Def. $\psi(x) := \sum_{p^k \le x} \log(p) = \sum_{n \le x} \Lambda(n)$.
Seien $q, a \in \mathbb{Z}$, $q \ge 1$. Def. $\psi(x; q, a) := \sum_{\substack{p^k \le x \\ p^k \equiv a\ (q)}} \log(p) = \sum_{\substack{n \le x \\ n \equiv a\ (q)}} \Lambda(n)$.

2.7. **Bezeichnungen:** Man nennt ϑ die 1. Tschebyschev-Funktion, und ψ die 2. Tsch.-Fkt.
↖ kurz: "Tsch.-fkt."

2.8. **Trivial:** $\pi(x) \le x$, $\vartheta(x) \le x\log(x)$, $\psi(x) \le x\log(x)$,
$\pi(x;q,a) \le \lceil \frac{x}{q} \rceil$, $\vartheta(x;q,a) \le \lceil \frac{x}{q} \rceil \log(x)$, $\psi(x;q,a) \le \lceil \frac{x}{q} \rceil \log(x)$.

2.9. **Bem.:** a) $\pi(x;1,a) = \pi(x)$, ebenso für ϑ und ψ

b) ϑ und ψ unterscheiden sich wenig voneinander:
$\psi(x) = \vartheta(x) + O(\sqrt{x})$, (bzw. $O(\sqrt{x}\log x)$ ohne Tsch.)

c) $\psi(x;q,a) = \vartheta(x;q,a) + O(\sqrt{x})$, nicht triv. für $\varphi(q) = o(\sqrt{x})$.

Bew.: a): ✓, b): $\psi(x) - \vartheta(x) = \sum_{\substack{p^k \le x \\ k \ge 2}} \log(p) = \sum_{p \le \sqrt{x}} \log(p) \sum_{2 \le k \le \frac{\log(x)}{\log(p)}} 1$

$$\le \sum_{p \le \sqrt{x}} \log(p) \cdot \frac{x}{\log p} = \pi(\sqrt{x}) \log(x) \underset{\text{Tsch., s.u.}}{\ll} \sqrt{x}.$$

Wird im letzten Schritt die triviale Absch. $\pi(\sqrt{x}) \le \sqrt{x}$ verwendet, erhält man $\psi(x) - \vartheta(x) \ll \sqrt{x}\log(x)$, was meistens schon ausreicht.

c): analog: $\psi(x;q,a) - \vartheta(x;q,a) \le \sum_{p \le \sqrt{x}} \log(p) \sum_{k \le \frac{\log(x)}{\log(p)}} 1 \ll \sqrt{x}$.
(bzw. $\sqrt{x}\log(x)$ ohne Tsch.)

Trivial: $\vartheta(x;q,a) = \sum_{\substack{p \le x \\ p \equiv a (q)}} \log(p) \ll \frac{x}{q}\log(x)$, ebenso für $\psi(x;q,a)$

Auch: $\gg \frac{x}{\varphi(q)}$ → Für $\varphi(q) \ge \sqrt{x}$ ist Fehlerterm $O(\sqrt{x})$ größer als Hauptterm. □

laut späterem PZS in APs

2.10. **Satz (von Tschebyschev):** (← hier oft auch "Tsch." abgekürzt)

(a) $\exists C_1 < C_2$: $\forall x \ge 2$: $C_1 \frac{x}{\log(x)} \le \pi(x) \le C_2 \frac{x}{\log(x)}$ $\iff$ $\frac{x}{\log(x)} \ll \pi(x) \ll \frac{x}{\log(x)}$

(b) $\exists C_3 < C_4$: $\forall x \ge 2$: $C_3 x \le \psi(x) \le C_4 x$ $\iff$ $x \ll \psi(x) \ll x$

(c) $\exists C_5 < C_6$: $\forall x \ge 2$: $C_5 x \le \vartheta(x) \le C_6 x$ $\iff$ $x \ll \vartheta(x) \ll x$

Bew.: * Alle drei Aussagen sind äquivalent: (b)⇔(c) klar wegen 2.9. b) in der Form $\psi(x) = \vartheta(x) + O(\sqrt{x}\log x)$, (a)⇒(c) klar wegen $\vartheta(x) = \sum_{p \le x} 1 \cdot \log p \overset{P.S.}{=} \pi(x)\cdot\log x - \int_2^x \pi(t)\frac{dt}{t}$,

$\int_2^x \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \ll \sqrt{x} + \frac{x}{\log x}$

und $\int_2^x \frac{dt}{\log t} \ll \frac{x}{\log x}$, (c)⇒(a) wegen $\pi(x) = \sum_{p \le x} \frac{\log p}{\log p} \underset{P.S.}{=} \vartheta(x)\cdot\frac{1}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$,

und $\int_2^x \frac{dt}{(\log t)^2} = \int_2^{\sqrt{x}} \frac{dt}{(\log t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\log t)^2} \le \sqrt{x} + x\cdot\frac{1}{(\log\sqrt{x})^2} \ll \frac{x}{(\log x)^2}$.

$\pi(x) \begin{cases} \ge \frac{\vartheta(x)}{\log x} & ✓ \\ \ll \frac{\vartheta(x)}{\log x} & ✓ \end{cases}$

* Zeigten in Ant 11 noch $\vartheta(x) \le x\log(4)$, $\psi(x) \ge \frac{x}{\log(4)}$, genügt. □

2.11. Kor.: Bertrands Postulat: Sei $n \in \mathbb{N}$. Dann $\exists p: \; n < p \leq 2n$.

Bew.: OK für $n \leq \tilde{x}_0$ ✓, ansonsten: $\sum_{n<p\leq 2n} \log(p) = \vartheta(2n) - \vartheta(n) > n\Big(\underbrace{\tfrac{2}{\log(4)} - \log(4)}_{\approx 0.056 > 0}\Big)$. ✓ □

$\tilde{x}_0$ explizit berechenbar

2.12. Bekannte numerische Schranken [Rosser & Schoenfeld, 1975] für ϑ, π, ψ:

$$\vartheta(x) < 1.000081\, x, \quad x > 0$$

$$\vartheta(x) > 0.75\, x, \quad x \geq 36$$

$$\frac{1}{\log x} \leq \pi(x) \leq \frac{1.25506\, x}{\log(x)}, \quad \text{u.S.: } x \geq 17, \text{ o.S.: } x > 1$$

$$|\vartheta(x) - x| < \frac{8.686\, x}{\log^2(x)}, \quad x > 1$$

ebenso für ψ

Effektive Absch. für $\psi(x; q, a)$, $\vartheta(x; q, a)$, $\pi(x; q, a)$:

2.13. Satz von Dusart (2001):

Für $x > x_0(q)$, mit $x_0(q)$ effektiv berechenbar, gilt

$$\left|\psi(x; q, a) - \frac{x}{\varphi(q)}\right| < x \cdot \varepsilon(x), \quad \text{wo } \varepsilon(x) = \sqrt[4]{\frac{q^2 \log(x)}{R\, \varphi(q)^2}} \cdot \exp\left(-\sqrt{\frac{\log(x)}{R}}\right), \quad R \approx 9.646$$

ebenso für ϑ.

2.14. Bsp.: $\pi(x; 3, a) < \dfrac{0.55\, x}{\log(x)}, \quad x \geq 229\,869.$

$$\left|\theta(x; 3, a) - \frac{x}{2}\right| < \frac{0.262\, x}{\log x}, \quad x \geq 1531.$$

2.15. Eine Vermutung von Gauß (1849) besagte: $\pi(x) \sim li(x) := \int_2^x \frac{dt}{\log(t)}$ (li heißt logarithmisches Integral) und ist heute bewiesen und bekannt als

"Primzahlsatz"

PZS (1896, Hadamard / de la Vallée-Poussin): $\boxed{\pi(x) \sim \dfrac{x}{\log(x)}.}$

2.16. Bem.: • Jeder analytische Beweis des PZSes benutzt die trigonometrische Unglg.

$$3 + 4\cos(\alpha) + \cos(2\alpha) \geq 0 \quad \text{denn: l.S.} = 2(1 + \cos\alpha)^2.$$

• Wegen 2.9.b) sind auch $\vartheta(x) \sim x$ und $\psi(x) \sim x$ zum PZS äquivalent.

2.17. Die beiden in 2.15 genannten PZS-Versionen sind äquivalent, weil $li(x) \sim \frac{x}{\log(x)}$ gilt:

Haben $li(x) = \int_2^x \frac{dt}{\log t} = \int_2^x \underbrace{1}_{u'} \cdot \underbrace{\frac{1}{\log t}}_{v} \cdot dt \overset{p.I.}{=} \frac{t}{\log t}\Big|_2^x + \int_2^x \frac{t}{t\log^2 t}\,dt = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} + O(1)$

mit $\int_2^x \frac{dt}{\log^2(t)} = \int_2^{\sqrt{x}} \frac{dt}{\log^2(t)} + \int_{\sqrt{x}}^x \frac{dt}{\log^2(t)} = O(\sqrt{x}) + O\left(\frac{x}{\log^2(x)}\right) = O\left(\frac{x}{\log^2(x)}\right)$,

so dass $li(x) = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right)$ folgt. Weiter: $li(x) = \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + O\left(\frac{x}{\log^3(x)}\right)$, ...
Mit $\pi(x) \sim \frac{x}{\log(x)}$ folgt dann auch $\pi(x) \sim li(x)$. (vgl. Anz 12.5)

2.18. Die <u>bessere Approximation</u> liefert die Version: $\boxed{\pi(x) \sim li(x)}$,
<u>numerische Daten</u> zeigen dies deutlich. Die Version $\pi(x) \sim \frac{x}{\log(x)}$ kann wegen $\frac{x}{\log(x)} = li(x) + O\left(\frac{x}{\log^2(x)}\right)$ daher nur auf die Approximation $\pi(x) = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right)$ gebracht werden, eine weitere Verschärfung des Fehlerterm $O\left(\frac{x}{\log^2(x)}\right)$ ist nicht möglich.
Wie gut hingegen die Approximation $\pi(x) \sim li(x)$ ist,
ist eines der wichtigsten zentralen ungelösten Probleme der Mathematik:

2.19. <u>Riemannsche Vermutung</u> $\Leftrightarrow$ $\pi(x) - li(x) = O(\sqrt{x}\log(x))$.
Genauer: 1) $(RH) \Rightarrow \pi(x) = li(x) + O(\sqrt{x}\log(x))$, 2) $\forall \varepsilon > 0: \pi(x) = li(x) + O(x^{1/2+\varepsilon}) \Rightarrow (RH)$.
Wir werden noch sehen, dass die (RH) die folgende analytische Formulierung hat:
"Jede nichttriviale Nullstelle von ζ im Streifen $0 \le \sigma \le 1$ hat den Realteil $\frac{1}{2}$."
Dass ζ etwas mit Primzahlen zu tun hat, ist bereits an der Formel $-\frac{\zeta'}{\zeta}(s) = \sum_{n \ge 1} \frac{\Lambda(n)}{n^s}$ zu sehen.

2.20. Das bis heute beste Ergebnis zum Fehlerterm im PZS lautet:
<u>PZS mit Restglied</u> (nach <u>Vinogradov/Korobov 1958</u>):

$$\pi(x) = li(x) + O\left(\frac{x}{\exp(c_1 (\log x)^{3/5} (\log\log x)^{-1/5})}\right) \text{ für eine Konstante } 0 < c_1 < 1.$$

2.21. Mit nicht allzu komplizierten Mitteln werden wir bereits das Fehlerglied $O\left(\frac{x}{\exp(c_2\sqrt{\log x})}\right)$ beweisen, was wir als <u>"1. Version"</u> des PZSes mit Restglied bezeichnen. Darüberhinaus zeigen wir auf, wie sich die <u>"2. Version"</u>, nämlich die Vinogradov/Korobov-Version zeigen lässt (voraussichtlich nicht in allen Details).

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a3: Dirichletreihen, Perronsche Formel

Stichworte: Dirichletreihen, ihr Konvergenzverhalten, Zusammenhang mit zahlentheoretischen Funktionen, Koeffizientensumme, Perronsche Formel

---

3.1. Einleitung: Wir wiederholen die wichtigsten Eigenschaften von Dirichletreihen. Ein zentrales Werkzeug zur Auffindung einer asymptotischen Formel für die Koeffizientensumme einer Dirichletreihe ist die Perronsche Formel, welche auch Abschätzungen des Restterms in der Asymptotik liefern kann.

3.2 Def: Eine Dirichletreihe ist eine unendl. Reihe der Form $D(s)=\sum_{n\geq 1} a_n n^{-s}$, die $a_n \in \mathbb{C}$, $s\in\mathbb{C}$. ($s=\sigma+it$)
Es stellt sich die Frage nach dem Konvergenzbereich.

3.3. Satz (Kgz. trichter): Es sei $D(s)$ in einem Pkt. s_0 konvergent. Dann konvergiert $D(s)$ gleichmäßig in dem Winkelraum / Konvergenztrichter $|\arg(s-s_0)|<\frac{\pi}{2}-\delta$ für festes $\delta>0$. Die Fkt. $D(s)$ ist demnach in $\{\sigma>\sigma_0\}$ holomorph.
Bew.: s. AnZ 4.4.

3.4. Satz: Zu jeder Dirichletreihe $D(s)$ gibt es stets ein $\sigma_c\in\mathbb{R}\cup\{\pm\infty\}$, so dass $D(s)$ für alle $s=\sigma+it$ mit $\sigma>\sigma_c$ kgt., und für $\sigma<\sigma_c$ div.
Zu $D(s)$ existiert auch stets ein $\sigma_a\in\mathbb{R}\cup\{\pm\infty\}$, so dass $D(s)$ für alle $s=\sigma+it$ mit $\sigma>\sigma_a$ absolut kgt., und für $\sigma<\sigma_a$ nicht.
Man hat, falls $\sigma_c\in\mathbb{R}$, $\sigma_c\leq\sigma_a\leq\sigma_c+1$ (*). Bew.: AnZ 4.7.

Hinweis zu (*): Ist $\sum a_n n^{-s_1}$ bei s_1 kgt., dann ist $(a_n n^{-s_1})$ beschr., etwa durch B. Für $\varepsilon>0$ ist $\sum|a_n n^{-s_1-1-\varepsilon}|\leq B\sum n^{-1-\varepsilon}$, d.h. absolute Kgz. bei $s_1+1+\varepsilon$.

3.5. Def.: σ_c heißt Konvergenzabszisse, σ_a heißt absolute Konvergenzabszisse von $D(s)$.

3.6. Satz von Landau: Ist σ_c die Kgz.abszisse von $F(s)=\sum a_n n^{-s}$ und $\forall n: a_n\geq 0$, dann ist F nicht in $s=\sigma_c$ holomorph fortsetzbar. (z.B. ist ζ nicht in $s=1$ hol. fortsetzbar)
Bew.: s. AnZ 7.

3.7. **Identitätssatz:** Seien $F(s)=\sum a_n n^{-s}$, $G(s)=\sum b_n n^{-s}$ kgt. für $\sigma>\sigma_c$.
Es gebe eine Folge $(s_m)=(\sigma_m+i\tau_m)_{m\in\mathbb{N}}$ mit $\sigma_m \xrightarrow{m\to\infty} \infty$ und
$\forall m\in\mathbb{N}: F(s_m)=G(s_m)$. Dann gilt $\forall m\in\mathbb{N}: a_m=b_m$. Bew.: AnZ 4.12.

Bem.: Dieser Satz wird in der Literatur gelegentlich falsch wiedergegeben. Es genügt nicht, eine Übereinstimmung von F und G auf Kompakta vorauszusetzen.

3.8. **Multiplikationssatz:** Seien $F(s)=\sum a_n n^{-s}$, $G(s)=\sum b_n n^{-s}$ abs. kgt. (in s). Dann hat $H(s)=F(s)G(s)$ die Gestalt $H(s)=\sum c_n n^{-s}$ mit $c_n=\sum_{d|n} a_d b_{n/d}$ (d.h. $c=a*b$).
Die Reihe $\sum c_n n^{-s}$ kgt. ebenfalls absolut (in s).

Bew.: Nach dem Produktsatz für Reihen und der vorausgesetzten abs. kgz. kann $F(s)G(s)$ ausmultipliziert und in beliebiger Anordnung aufsummiert werden:
$$F(s)G(s)=\sum_{n,m} a_n b_m (nm)^{-s} = \sum_k k^{-s} \sum_{nm=k} a_n b_m = \sum_k c_k k^{-s}. \qquad \square$$

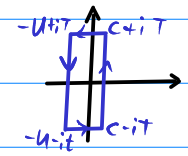
3.9. **Def.:** zahlentheoretische Funktion: Funktion $A:\mathbb{N}\to\mathbb{C}$ bzw. komplexwertige Folge (a_n).
Dirichlet-Produkt zweier zth. Fktn. a und b ist $a*b=c$ mit $c_n=\sum_{d|n} a_d b_{n/d}$.
ihre erzeugenden Dirichletreihen: $A(s)=\sum a_n n^{-s}$, $B(s)=\sum b_n n^{-s}$.

3.10. **Satz:** Die zth. Fktn. bilden mit $*$ eine abelsche Halbgruppe mit Einselement ε, $\varepsilon(n)=\lfloor \frac{1}{n}\rfloor$.
"1-Erkennungsfkt."
Die zth. Fktn. f mit $f(1)\neq 0$ " " " Gruppe.
Die Möbiusfunktion $\mu(n)=\begin{cases}(-1)^r, & n=p_1\cdots p_r \text{ mit p.w.v. } p_1,\dots,p_r \text{ prim},\\ 1, & n=1,\\ 0, & \text{sonst, d.h. } \exists p \text{ prim}: p^2|n\end{cases}$
ist Faltungsinverse der Fkt. $\mathbb{1}(n)=1$ d.h. $\mu*\mathbb{1}=\varepsilon$.
"Möbiussche Umkehrformel"
Bew.: AnZ 2.3.

In Anwendungen kommt es oft vor, dass man von den analytischen Eigenschaften einer Dirichletreihe $\sum_{n\geq 1} a_n n^{-s}$ auf ihre Koeffizientensumme $\sum_{n\leq x} a_n$ schließen will. Die Funktionentheorie liefert gute Werkzeuge dafür; ein neues und wichtiges erarbeiten wir jetzt.

Zur Vorbereitung zunächst folgendes Hilfsergebnis zu komplexen Integralen:

3.11. **Lemma:** Es seien $c,T,y>0$. Dann ist für $T\to\infty$:
$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds = \begin{cases} 1+O(y^c T^{-1}|\log(y)|^{-1}), & \text{falls } y>1,\\ O(y^c T^{-1}|\log(y)|^{-1}), & \text{falls } 0<y<1. \end{cases} \qquad (y\neq 1)$$



Bew.: • Sei $y>1$. Für $u>0$ zeigt der Residuensatz:

$$\frac{1}{2\pi i}\left(\int_{-u-it}^{c-iT}+\int_{c-iT}^{c+iT}+\int_{c+iT}^{-u+iT}+\int_{-u+iT}^{-u-iT}\right)\frac{y^s}{s}\,ds = \operatorname{Res}_{s=0}\left(\frac{y^s}{s}\right)=1.$$

$y^s=\exp(s\log(y))=1+\frac{s\log(y)}{1}+\frac{s^2\log^2(y)}{2!}+\dots$

• Haben $\left|\left(\int_{c+iT}^{-u+iT}+\int_{-u-iT}^{c-iT}\right)\frac{y^s}{s}\,ds\right|\le\frac{1}{T}\int_{-\infty}^{c}y^\sigma d\sigma=O\left(y^cT^{-1}|\log(y)|^{-1}\right)$

und $\left|\int_{-u-iT}^{-u+iT}\frac{y^s}{s}\,ds\right|=O\left(Ty^{-u}|\log(y)|^{-1}\right)\xrightarrow[y>1]{u\to\infty}0$. Es folgt: $\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{y^s}{s}\,ds=1+O\left(y^cT^{-1}|\log(y)|^{-1}\right)$.

• Sei $0<y<1$. Nach dem Cauchyschen $\int$-Satz ist

$$\frac{1}{2\pi i}\left(\int_{u-it}^{c-iT}+\int_{c-iT}^{c+iT}+\int_{c+iT}^{u+iT}+\int_{u+iT}^{u-iT}\right)\frac{y^s}{s}\,ds=0.$$

Wie oben gilt $\left|\left(\int_{c+iT}^{u+iT}+\int_{u-iT}^{c-iT}\right)\frac{y^s}{s}\,ds\right|\le\frac{1}{T}\int_{c}^{\infty}y^\sigma d\sigma=O\left(y^cT^{-1}|\log(y)|^{-1}\right)$

und $\left|\int_{u-iT}^{u+iT}\frac{y^s}{s}\,ds\right|=O\left(Ty^{u}|\log(y)|^{-1}\right)\xrightarrow[0<y<1]{u\to\infty}0$. Es folgt die Beh. $\square$

Die Koeffizientensumme einer Dirichletreihe erhalten wir damit wie folgt:

3.12. Satz (Perronsche Formel):

Es sei $D(s)=\sum_{n\ge1}a_nn^{-s}$ für $\sigma>1$ abs. kgt. Mit einer für $x\ge x_0$ mon. w. positiven Fkt. $\Phi(x)$ und einer Konstanten $C>0$ sei $|a_n|<C\cdot\Phi(x)$ für alle $n\le x$.
Es sei $\sum_{n\ge1}|a_n|n^{-\sigma}=O\left((\sigma-1)^{-\alpha}\right)$ bei $\sigma\to1+$ für ein festes $\alpha>0$,
sowie $c>1$, $x>1$, $x\notin\mathbb{Z}$, $T>0$. Dann gilt

$$\sum_{n\le x}a_n=\frac{1}{2\pi i}\int_{c-iT}^{c+iT}D(s)\frac{x^s}{s}\,ds+$$
$$+O\left(\frac{x^c}{T(c-1)^\alpha}\right)+O\left(\frac{x\,\Phi(2x)\log(2x)}{T}\right)+O\left(\frac{x\,\Phi(2x)}{T\cdot\|x\|}\right)\quad\text{für } T\to\infty,$$

wobei $\|x\|:=\min\{|x-z|;\,z\in\mathbb{Z}\}$ der Abstand von x zur nächsten ganzen Zahl ist.

Bew. von Satz 3.12 (Perronsche Formel):

Da $\sum_{n\geq 1} a_n n^{-s}$ glm. auf $[c-iT, c+iT]$ kgt., zeigt Lemma 3.11, dass

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} D(s)\frac{x^s}{s}\,ds = \sum_{n\geq 1} a_n\left(\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^s ds\right) = \sum_{n<x} a_n + O\Big(\frac{x^c}{T}\underbrace{\sum_{n\geq 1}\frac{|a_n|}{n^c\left|\log\left(\frac{x}{n}\right)\right|}}_{=:\Sigma_0}\Big).$$

Spalte Σ_0 auf in $\Sigma_0 = \Sigma_1 + \Sigma_2 + \Sigma_3$ mit $\Sigma_1 = \sum_{n<x/2}\dots$, $\Sigma_2 = \sum_{n>2x}\dots$, $\Sigma_3 = \sum_{\frac{x}{2}\leq n\leq 2x}\dots$

- Für $n<\frac{x}{2}$ oder $n>2x$ ist $\left|\log\left(\frac{x}{n}\right)\right| > \log(2)$,
  also $\Sigma_1 + \Sigma_2 = O\left(\sum_{n\geq 1}|a_n| n^{-c}\right) = O\left((c-1)^{-\alpha}\right)$ nach Vor. ✓

- Absch. von Σ_3: Sei $N\in\mathbb{N}$ so, dass $|x-N| = \|x\|$. Für $N<n\leq 2x$ sei $r := n-N$.
  Wegen $x\leq N+\frac{1}{2}$ gilt $\log\left(\frac{n}{x}\right) \geq \log\left(\frac{N+r}{N+1/2}\right) = \log\left(1+\frac{r-1/2}{N+1/2}\right)$.
  Laut MWS ist $\log(1+u)\geq c_0 u$ für $0\leq u\leq 1$,
  und $\log\left(1+\frac{r-1/2}{N+1/2}\right) \geq c_0\frac{r-1/2}{N+1/2} \geq c_1\cdot\frac{r}{x}$, wo $c_0, c_1>0$ feste Konstanten.

Also: $$\sum_{N<n\leq 2x}\frac{|a_n|}{n^c\left|\log\left(\frac{x}{n}\right)\right|} = O\Big(\Phi(2x)\,x^{1-c}\sum_{1\leq r\leq 2x}\frac{1}{r}\Big) = O\big(\Phi(2x)\,x^{1-c}\log(2x)\big).$$

Genauso: $$\sum_{x/2\leq n<N}\frac{|a_n|}{n^c\left|\log\left(\frac{x}{n}\right)\right|} = O\big(\Phi(2x)\,x^{1-c}\log(2x)\big),$$ und für $n=N$ ist

$$\frac{|a_N|}{N^c\left|\log(x/N)\right|} = O\left(\frac{\Phi(N)}{N^c\left|\log\left(1+\frac{x-N}{N}\right)\right|}\right) = O\left(\frac{\Phi(2x)\,x^{1-c}}{\|x\|}\right).$$

□

3.13. **Bem.:** Die Perronsche Formel ist ein wichtigstes Werkzeug, um aus den analytischen Eigenschaften einer Dirichletreihe auf die Asymptotik bzw. Abschätzung der Koeffizientensumme $\sum_{n\leq x} a_n$ zu schließen.
Eine wichtige Anwendung ist bereits der Fall der 2. Tsch.-Fkt.
$\psi(x) = \sum_{n\leq x}\Lambda(n)$, die zur Dirichletreihe $\sum_{n\geq 1}\Lambda(n)n^{-s} = -\frac{\zeta'}{\zeta}(s)$ gehört.

Beachten $\left(\sum_n \Lambda(n)n^{-s}\right)\left(\sum_m m^{-s}\right) = \sum_k (\Lambda * \mathbb{1})(k)\,k^{-s} = \sum_k (\log k)\cdot k^{-s} = -\zeta'(s)$ für $\sigma>1$.

Die Nullstellen des Nenners $\zeta(s)$ sind die Pole von $\frac{\zeta'}{\zeta}(s)$, die laut Residuensatz zum $\int$ der Perronformel beitragen.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a4: Nullstellenanzahlen

Stichworte: Perronsche Formel auf $-\frac{\zeta'}{\zeta}$ angewendet, Satz von Borel-Carathéodory, Größenordnung von ζ, Anzahl $N(T)$ im kritischen Streifen

---

4.1. Einleitung: Wir untersuchen nun, welche Konsequenzen die Anwendung der Perronschen Formel auf die Identität

$$(*) \qquad -\frac{\zeta'}{\zeta}(s) = \sum_{n\geq 1} \Lambda(n) n^{-s} \quad \text{für } \sigma > 1 \qquad \text{hat,}$$

und was zum Beweis eines PZSes mit Restglied noch erforderlich ist. Mit der Abschätzung der Größenordnung von ζ finden wir eine Abschätzung für die Anzahl der ζ-Nullstellen in Rechtecken des kritischen Streifens.

4.2. Lemma: Es sei $x = m + \frac{1}{2}$ für $m \in \mathbb{N}$ und $c = c(x) = 1 + \frac{1}{\log(x)}$. Dann ist

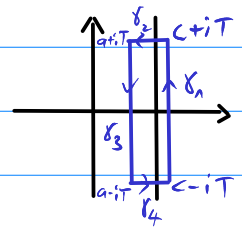
$$\psi(x) = \int_{c-iT}^{c+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \cdot \frac{x^s}{s}\, ds + O\left(\frac{x \log^2(x)}{T}\right).$$

Bew.: Wende die Perronsche Formel Satz 3.12 an mit $a_n = \Lambda(n)$ auf $(*)$ mit der Koeffizientenbeschränkung $\Phi(x) = \log(x)$.
Da $D(s) = -\frac{\zeta'}{\zeta}(s)$ einen Pol 1. Ordnung in $s = 1$ besitzt, folgt

$$\sum_{n\geq 1} \Lambda(n) n^{-\sigma} = O\left((\sigma-1)^{-1}\right), \quad \sigma \to 1^+.$$

Können in Satz 3.12 $\alpha = 1$ wählen. Die drei Fehlerterme darin sind alle durch $O\left(\frac{x}{T}\log^2(x)\right)$ beschränkt. $\square$

Im folgenden ergänzen wir den Integrationsweg $[c-iT, c+iT]$ zu einer geschlossenen Kurve, die ein Rechteck R im positiven Sinne berandet: $\gamma = [c-iT, c+iT] \cup [c+iT, a+iT] \cup [a+iT, a-iT] \cup [a-iT, c-iT]$, $a<1<c$.



Die einzige in R enthaltene Singularität von $\frac{\zeta'}{\zeta}$ soll $s=1$ sein, so dass das $\int$ durch den Residuensatz ausgewertet werden kann. Dazu muss die Nullstellenfreiheit von ζ in R sichergestellt sein.

Ergebnisse aus AnZ: $\zeta(s) \neq 0$ für $\sigma > 1$,

und $\zeta(s) \neq 0$ für $\sigma = 1$ (Hadamard/de la Vallée-Poussin).

Dies reicht nur, um die Asymptotik im PZS zu zeigen. Um eine Version mit Fehlerterm zu erhalten, müssen wir die Existenz eines nullstellenfreien Gebietes im kritischen Streifen zeigen.

Dafür stellen wir einige Hilfsmittel aus der Funktionentheorie bereit.

43. **Satz (Borel–Carathéodory):** Die Fkt. f sei holomorph auf einem Gebiet, das $|s| \le R$ enthält. Sei $f(0)=0$ und $\operatorname{Re} f(s) \le M$ für alle $|s| \le R$. Dann gilt für $|s| \le r < R$ die Abschl. $|f(s)| \le \frac{2Mr}{R-r}$, $|f'(s)| \le \frac{2MR}{(R-r)^2}$.

Bew.: • Zeige zunächst: $\left|\frac{f^{(k)}(0)}{k!}\right| \le \frac{2M}{R^k}$ für alle $k \ge 1$. ⊛

⌈ Subst. $s = Re(\theta)$ gibt mit Cauchy-Ş-formel $\qquad (e(\theta) := e^{2\pi i\theta})$

$$\int_0^1 f(Re(\theta))\,d\theta = \frac{1}{2\pi i}\int_{|s|=R} f(s)\frac{ds}{s} = f(0) = 0.$$

Für $k>0$ ist $\int_0^1 f(Re(\theta))\,e(k\theta)\,d\theta = \frac{R^{-k}}{2\pi i}\int_{|s|=R} f(s)\,s^{k-1}\,ds = 0$

und $\int_0^1 f(Re(\theta))\,e(-k\theta)\,d\theta = \frac{R^k}{2\pi i}\int_{|s|=R} f(s)\,s^{-k-1}\,ds = \frac{R^k f^{(k)}(0)}{k!}$.

Durch Linearkomb. folgt für $\phi \in \mathbb{R}$ bel.

$$\int_0^1 f(Re(\theta))\,(1+\cos(2\pi(k\theta+\phi)))\,d\theta = \frac{R^k}{2k!}\cdot e(-\phi)\,f^{(k)}(0)$$

und $\operatorname{Re}\left(\frac{R^k}{2k!}e(-\phi)\,f^{(k)}(0)\right) \le M\int_0^1 (1+\cos(2\pi(k\theta+\phi)))\,d\theta = M$

für alle $k>0$. Wähle ϕ so, dass $e(-\phi)\,f^{(k)}(0) = |f^{(k)}(0)|$. Es folgt ⊛. ⌋

• Aus ⊛ folgt $|f(s)| \le \sum_{k\ge1}\left|\frac{f^{(k)}(0)}{k!}\right| r^k \le 2M\sum_{k\ge1}\left(\frac{r}{R}\right)^k = \frac{2Mr}{R-r}$

und $|f'(s)| \le \sum_{k\ge1}\left|\frac{f^{(k)}(0)}{k!}\right| k r^{k-1} \le \frac{2M}{R}\sum_{k\ge1} k\left(\frac{r}{R}\right)^{k-1} = \frac{2MR}{(R-r)^2}$. □

4.4. **Lemma:** Sei f holom. in Gebiet, das $|s-s_0|\le r$ umfasst. Sei $M>1$ so, dass $\left|\frac{f(s)}{f(s_0)}\right|<e^M$ auf $|s-s_0|\le r$ gilt. Dann ex. $A>0$ mit

$$\left|\frac{f'(s)}{f(s)}-\sum_{\varrho}\frac{1}{s-\varrho}\right|<\frac{AM}{r} \quad \text{für } |s-s_0|\le\frac{r}{4},$$

wobei ϱ die Nullst. von f in $|s-s_0|\le\frac{r}{2}$ (mit Vielfachheiten) durchläuft.

Bew.: Setze $g(s)=f(s)\cdot\prod_{\varrho}\frac{1}{s-\varrho}$, ist für $|s-s_0|\le r$ hol., auf $|s-s_0|\le\frac{r}{2}$ ist $g\neq 0$.
Auf dem Rand $|s-s_0|=r$ gilt $|s-\varrho|\ge\frac{r}{2}\ge|s_0-\varrho|$,
also $\left|\frac{g(s)}{g(s_0)}\right|=\left|\frac{f(s)}{f(s_0)}\right|\cdot\left|\prod_{\varrho}\frac{s_0-\varrho}{s-\varrho}\right|\le\left|\frac{f(s)}{f(s_0)}\right|\underset{\text{Vor.}}{\le}e^M$,
nach dem Maximumsprinzip gilt dies auch für $|s-s_0|\le r$.
Setze $h(s)=\mathrm{Log}\left(\frac{g(s)}{g(s_0)}\right)$, wo Log die anal. Fkt. von $\log:(0,\infty)\to\mathbb{R}$ sei.
Dann ist h hol. für $|s-s_0|\le\frac{r}{2}$. Weiter ist $h(s_0)=0$ und $\mathrm{Re}\,h(s)\le M$.
Nach Satz 4.3 von Borel-Carathéodory ist $|h'(s)|\le\frac{2M\cdot r/2}{(r/2-r/4)^2}\le\frac{AM}{r}$ für $|s-s_0|\le\frac{r}{4}$. □

4.5 **Lemma:** Sei f holom. in Gebiet, das $|s-s_0|\le r$ umfasst. Sei $M>1$ so, dass $\left|\frac{f(s)}{f(s_0)}\right|<e^M$ auf $|s-s_0|\le r$ gilt, und f habe keine Nullst. im Halbkreis $\{|s-s_0|\le r;\ \mathrm{Re}\,s>\mathrm{Re}\,s_0\}$.

(i) Dann gilt $-\mathrm{Re}\,\frac{f'(s_0)}{f(s_0)}<\frac{AM}{r}$. (Für $A>0$ aus Lemma 4.4.)

(ii) Hat f eine Nullst. ϱ_0 auf der Strecke $[s_0-\frac{r}{2},s_0)$, dann ex. $A>0$ mit $-\mathrm{Re}\,\frac{f'(s_0)}{f(s_0)}<\frac{AM}{r}-\frac{1}{s_0-\varrho_0}$.

Bew.: Aus Lemma 4.4 folgt $-\mathrm{Re}\,\frac{f'(s_0)}{f(s_0)}<\frac{AM}{r}-\underbrace{\sum_{|\varrho-s_0|\le r/2}\mathrm{Re}\,\frac{1}{s_0-\varrho}}_{\text{in (ii): behalte nur den einen Summanden } \mathrm{Re}\frac{1}{s_0-\varrho_0}=\frac{1}{s_0-\varrho_0}}$. Aus $\mathrm{Re}\,\frac{1}{s_0-\varrho}\ge 0$ für alle ϱ in der Σ folgt die Beh. (i). □

4.6. **Lemma (einfache O.S. für ζ):** Es sei $m \in \mathbb{Z}$, $\delta > 0$. Für $\sigma = -m + \delta$, $|s-1| \geq 1$ ist $\zeta(s) = O_{m,\delta}(t^{m+1})$ für $|t| \to \infty$.

Bew.: Nach der allg. Eulerschen Σ-Formel Satz 4.7 für ζ mit $\sigma > 1$, $\varepsilon < \frac{1}{2}$,

$g(u) = u^{-s}$, $g^{(k)}(u) = (-1)^k s(s+1)\cdots(s+k-1)u^{-(s+k)}$ ist

$$\zeta(s) = \lim_{x\to\infty}\left(\int_{1-\varepsilon}^{x} g(u)\,du + \sum_{k=0}^{m}(-1)^{k+1}\left(g^{(k)}(x)P_k(x) - g^{(k)}(1-\varepsilon)P_k(1-\varepsilon)\right) + (-1)^m\int_{1-\varepsilon}^{x} g^{(m+1)}(u)P_m(u)\,du\right)$$

$$\xrightarrow{\varepsilon\to 0+} \lim_{x\to\infty}\left(\frac{1}{s-1} + \frac{1}{2} - P_0(x)x^{-s} + \sum_{k=1}^{m}(-1)^{k+1}s(s+1)\cdots(s+k-1)\cdot\left(x^{-(s+k)}P_k(x) - P_k(1)\right)\right)$$
$$+ (-1)^m s(s+1)\cdots(s+m)\int_1^\infty u^{-(s+m+1)}P_m(u)\,du$$

$$= \frac{1}{s-1} + \frac{1}{2} + \sum_{k=1}^{m}(-1)^k P_k(1)\,s(s+1)\cdots(s+k-1)$$
$$+ (-1)^m s(s+1)\cdots(s+m)\underbrace{\int_1^\infty u^{-(s+m+1)}P_m(u)\,du}_{\text{konv. für } \sigma > -m}.$$

$\rightsquigarrow$ Darst. gilt für $\sigma > -m$.

Haben: $\int_1^\infty u^{-(s+m+1)}P_m(u)\,du = O(1)$.

Für $1 \leq k \leq m+1$ ist $s(s+1)\cdots(s+k-1) = O_m(|t|^k)$, $|t| \to \infty$. $\square$

4.7. Satz 1.6 war nur die einfache Version der Euler Σ-Formel. Hier wird die allg. Euler-Maclaurin-Σ-Formel benutzt [mit $P_k(x) = \frac{B_{k+1}}{(k+1)!}(x - \lfloor x \rfloor)$, $B_0(x) = 1$, $B_k'(x) = k\,B_{k-1}(x)$.]

Für $m = 0$ enthält diese als Spezialfall die einfache Euler-Σ-Formel.

Der Beweis der Euler-Maclaurin-Σ-Formel ist genauso durch Nachrechnen möglich.

4.8. **Def.:** Sei $T > 0$. Mit $N(T)$ bezeichne die Anz. der Nullst. von ζ mit $0 < \mathrm{Re}(s) < 1$ und $0 < \mathrm{Im}(s) < T$.

4.9. **Lemma:** Es ist $N(T+1) - N(T) = O(\log(T))$ für $T \to \infty$.

Für $m \in \mathbb{N}$ und $s = \sigma + it$ mit $\sigma \geq -m$, $t > 0$, $\zeta(s) \neq 0$ gilt

$$\frac{\zeta'}{\zeta}(s) = \sum_{|\mathrm{Im}(\rho) - t| \leq 1}\frac{1}{s-\rho} + O_m(\log(t)), \quad t \to \infty.$$

(t groß)

Bew.: Wende Lemma 4.4 an mit $f=\zeta$, $s_0 = 2+it$, $r = 4(m+3)$.

Es ist $|\zeta(s_0)| = \prod_p \frac{1}{|1-p^{-s_0}|} \geq \prod_p \frac{1}{1+p^{-2}} \gg 1$.

Nach Lemma 4.6 sind die Vor. von Lemma 4.4 mit $M = 4(m+3)\log(t)$ erfüllt, falls $t \geq t_0$ hinr. groß. Für $|s-s_0| \leq \underbrace{m+3}_{=r/4}$ erhalten wir dann

$$\left|\frac{\zeta'}{\zeta}(s) - \sum_{\varrho} \frac{1}{s-\varrho}\right| = O_m(\log(t)), \quad (*)$$

wo ϱ alle Nst. von ζ mit $|\varrho - s_0| \leq 2(m+3)$ entsprechend Vielfachheit durchläuft.

Wende $(*)$ mit $s=s_0$, $m=2$ an: Mit $\frac{\zeta'}{\zeta}(s_0) = O(1)$ für $t\to\infty$ (L. 4.6, $m=-1$) folgt

$$\mathrm{Re}\left(\sum_{|\varrho-s_0|\leq 10} \frac{1}{s_0-\varrho}\right) = O(\log(t)). \quad (+)$$

Für $\varrho = \beta + i\gamma$ ist $\mathrm{Re}\left(\frac{1}{s_0-\varrho}\right) = \mathrm{Re}\left(\frac{\bar{s}_0-\bar{\varrho}}{|s_0-\varrho|^2}\right) = \frac{2-\beta}{|s_0-\varrho|^2}$.

Es ist $2-\beta \geq 1$, $|s_0-\varrho|^2 \leq 100$, also $\mathrm{Re}\left(\frac{1}{s_0-\varrho}\right) \geq \frac{1}{100}$ $\underset{(+)}{\Rightarrow}$ $N(t+1)-N(t) = O(\log(t))$.

Aus $(*)$ folgt für $|s-s_0| \leq m$ die Absch.

$$\left|\frac{\zeta'}{\zeta}(s) - \sum_{\substack{|\mathrm{Im}(\varrho)-t|\leq 1 \\ |\varrho-s_0|\leq 2(m+3)}} \frac{1}{s-\varrho}\right| = O_m(\log(t)) + O_m\Big(\sum_{|\mathrm{Im}(\varrho)-t|>1} \frac{1}{s-\varrho}\Big) = O_m(\log(t))$$

$\rightsquigarrow |s-\varrho| \geq |\mathrm{Im}(\varrho)-t| > 1$

wegen $N(t+1)-N(t) = O(\log(t))$.

$$\ll \sum_{1\leq m\leq 2m+3} \sum_{\substack{\varrho: \\ t+m \leq \mathrm{Im}(\varrho) \leq t+m+1}} \frac{1}{s-\varrho} \qquad \square$$

Anz. Summ. ist $\ll_m \log(t)$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a5: Primzahlsatz mit Restglied

Stichworte: nullstellenfreies Gebiet mit Größenordnung von ζ (1. Version), PZSatz mit Restglied (1. Version)

5.1. Einleitung: Wir zeigen zunächst ein allgemeines Ergebnis zum unmittelbaren Zusammenhang zwischen der Größenordnung von ζ nahe $\sigma=1$ und der Breite des nullstellenfreien Gebiets von ζ. Mit einem Die Größenordnung von ζ, die durch Lemma 4.6 gegeben ist, liefert ein passendes nullstellenfreies Gebiet und sofort die 1. Version des PZSs mit Restglied.

5.2. Satz (allg. Ergebnis zum nullst. freien Gebiet von ζ): Es ex. $A_1>0$:
Sei $\zeta(s) \ll e^{\Phi(t)}$ für $t\to\infty$ in $1-\theta(t)\le\sigma\le 2$, $t\ge 1$,
wobei $\Phi, \frac{1}{\theta}$ positiv und mon. w. in t, $\theta(t)\le 1$, $\Phi(t)\to\infty$, $\frac{\Phi(t)}{\theta(t)}e^{-\Phi(t)}\to 0$.
Es gelte zudem $\lim_{t\to\infty}\frac{\theta(t+1)}{\theta(t)} = \lim_{t\to\infty}\frac{\Phi(t+1)}{\Phi(t)} = 1$.
(i) Dann hat ζ keine Nullst. in dem Gebiet $\sigma \ge 1 - 2A_1\cdot\frac{\theta(2t+1)}{\Phi(2t+1)}$.
(ii) Außerdem gilt: $\sigma \ge 1 - A_1\cdot\frac{\Phi(2t)}{\theta(2t)} \Rightarrow \frac{\zeta'}{\zeta}(s) = O\left(\frac{\Phi(2t)}{\theta(2t)}\log(t)\right)$.

Bew.: Sei $\beta+i\gamma$ eine Nst. von ζ mit $\gamma>0$.
Sei σ_0 bel. mit $1+e^{-\Phi(2\gamma+1)}\le\sigma_0\le 2$, $s_0:=\sigma_0+i\gamma$, $s_0':=\sigma_0+2i\gamma$.
Sei $r=\theta(2\gamma+1)$. Da θ mon. f., liegen $|s-s_0|\le r$, $|s-s_0'|\le r$ in $\{\sigma+it \mid \sigma\ge 1-\theta(t)\}$. Da $\frac{1}{|\zeta(s_0)|}, \frac{1}{|\zeta(s_0')|} < \exp(A\Phi(2\gamma+1))$ für A hinr. gr., ex. $A_2>0$: $\left|\frac{\zeta(s)}{\zeta(s_0)}\right|, \left|\frac{\zeta(s)}{\zeta(s_0')}\right| < e^{A_2\Phi(2\gamma+1)}$ auf Kreisscheiben $|s-s_0|\le r$, $|s-s_0'|\le r$.
Wende Lemma 4.5 (i) an mit $M:=A_2\Phi(2\gamma+1)$,
ergibt $-\mathrm{Re}\left(\frac{\zeta'}{\zeta}(\sigma_0+2i\gamma)\right) < A_3\frac{\Phi}{\theta}(2\gamma+1)$. (1)
↳ auch mit σ_0+ir

Fall I: $\beta > \sigma_0 - 1/2$.

Wegen Lemma 4.5(ii) erhalten wir dann

$$-\mathrm{Re}\left(\frac{\zeta'}{\zeta}(\sigma_0+i\gamma)\right) < A_3 \frac{\Phi}{\theta}(2\gamma+1) - \frac{1}{\sigma_0-\beta}. \qquad (2)$$

Es ist $-\frac{\zeta'}{\zeta}(\sigma_0) < \frac{a}{\sigma_0-1}$ mit $a = a(\sigma_0) \xrightarrow{\sigma_0\to 1} 1$. (3)

Wie im Beweis von $\zeta(1+it)\neq 0$ nach dlV-P./H. verwenden wir nun die Unglg.

$$-3\frac{\zeta'}{\zeta}(\sigma_0) - 4\,\mathrm{Re}\frac{\zeta'}{\zeta}(\sigma_0+i\gamma) - \mathrm{Re}\frac{\zeta'}{\zeta}(\sigma_0+2i\gamma) \geq 0 \text{ für } \sigma>0.$$

⌜Denn: Wegen $-\frac{\zeta'}{\zeta}(s) = \sum_{n\geq 1}\Lambda(n)n^{-s}$ ist die l.S. $= \mathrm{Re}\left(\sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma_0}}(3+4n^{-i\gamma}+n^{-2i\gamma})\right)$

$$= \sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma_0}}\underbrace{\left(3+4\cos(-\gamma\log(n))+\cos(-2\gamma\log(n))\right)}_{\geq 0 \text{ wegen Bem. 2.16}}$$ ⌟

Mit obigem (1), (2) und (3) folgt $\frac{3a}{\sigma_0-1} + 5A_3\frac{\Phi}{\theta}(2\gamma+1) - \frac{4}{\sigma_0-\beta} \geq 0$,

also

$$\sigma_0-\beta \geq \left(\frac{3a}{4(\sigma_0-1)} + \frac{5A_3}{4}\cdot\frac{\Phi}{\theta}(2\gamma+1)\right)^{-1}, \text{ und somit:}$$

$$1-\beta \geq \left(\frac{3a}{4(\sigma_0-1)} + \frac{5A_3}{4}\cdot\frac{\Phi}{\theta}(2\gamma+1)\right)^{-1} - (\sigma_0-1) = \frac{1-3a/4-(5A_3/4)\cdot\frac{\Phi}{\theta}(2\gamma+1)\cdot(\sigma_0-1)}{\frac{3a}{4(\sigma_0-1)} + \frac{5A_3}{4}\cdot\frac{\Phi}{\theta}(2\gamma+1)}.$$

Für γ hinr. gr. wählen wir $\sigma_0 - 1 = \frac{1}{40A_3}\cdot\frac{\theta}{\Phi}(2\gamma+1)$ und $a = \frac{5}{4}$.

Erhalten $1-\beta \geq A_1\frac{\theta}{\Phi}(2\gamma+1)$, die Beh. (i).

Fall II: $\beta \leq \sigma_0 - \frac{1}{2} = 1 + \frac{1}{40A_3}\cdot\frac{\theta}{\Phi}(2\gamma+1) - \frac{\theta(2\gamma+1)}{2}$, woraus ebenso Beh. (i) folgt.

Mit Beh. (i) folgt für $\sigma \geq 1 - A_1\frac{\theta}{\Phi}(2t)$ die Absch. $|s-\rho|^{-1} \ll \frac{\Phi}{\theta}(2t)$ für alle Nullst. ρ von ζ mit $|\mathrm{Im}(\rho)-t| \leq 1$.

Mit Lemma 4.9 folgt Beh. (ii). □

Hatten:

4.6. **Lemma:** Sei $m \in \mathbb{Z}$ und $\delta > 0$. Für $\sigma = -m + \delta$ und $|s-1| \geq 1$ ist $\zeta(s) \ll_{m,\delta} t^{m+1}$ für $|t| \to \infty$.

[Speziell: $\zeta(s) \ll t$ in $0 < \sigma < 1$; man vergleiche 1.15]

Wir verwenden diese einfache Absch., um mit 5.2 eine einfache 1. Version über ein nullst. freies Gebiet von ζ und die 1. Version des PZSes mit Fehlerterm zu erhalten. Erst mit den Methoden des Kapitels a7 gelingt es, die Absch. von ζ (und damit das nullstellenfreie Gebiet und den PZSfehlerterm) noch weiter zu verbessern.

5.3. **Satz (nullstellenfreies Gebiet, 1. Version):** Es gibt ein $A_0 > 0$ mit $\zeta(s) \neq 0$ für $t \geq 0$ und $\sigma \geq 1 - \frac{2A_0}{\log(t)}$.
Für $\sigma \geq 1 - \frac{A_0}{\log(t)}$ gilt $\frac{\zeta'}{\zeta}(s) \ll \log^2(t)$.

Bew.: Wende Satz 5.2 an mit $\theta = \frac{1}{2}$.
Nach Lemma 4.6 ist die Vor. des Satzes erfüllt mit $\Phi(t) = C \cdot \log(t)$, d.h. haben $\zeta(s) \ll e^{\Phi(t)}$ für $t \to \infty$ im Streifen $1 - \theta(t) \leq \sigma \leq 2$, wo $C > 0$ fest. $\square$

5.4. **Satz (PZS mit Fehlerterm, 1. Version):** Ex. $c_0 > 0$: $\psi(x) = x + O\left(\frac{x}{\exp(c_0\sqrt{\log x})}\right)$.

Bew.: Sei $T = T(x) > 1$, $c = c(x) = 1 + 1/\log x$, $x = m + \frac{1}{2}$ mit $m \in \mathbb{N}$.
Wählen T später optimal. Nach Lemma 4.2 (Anw. der Perronschen Formel) ist $\psi(x) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(-\frac{\zeta'}{\zeta}\right)(s) \cdot \frac{x^s}{s} ds + O\left(\frac{x}{T} \log^2(x)\right)$.

Ergänzen den Integrationsweg $[c-iT, c+iT]$ zur geschlossenen Kurve
$\mathcal{C} = [c-iT, c+iT] \cup [c+iT, a+iT] \cup [a+iT, a-iT] \cup [a-iT, c-iT]$
mit $a = 1 - \frac{A_0}{\log(T)}$, wo A_0 die Konst. aus Satz 5.3 ist.

Nach Residuensatz und Satz 5.3 ist

$$\frac{1}{2\pi i}\int_{\mathcal{C}} \left(-\frac{\zeta'}{\zeta}\right)(s)\,\frac{x^s}{s}\,ds = \operatorname{Res}_1\left(-\frac{\zeta'}{\zeta}(s)\cdot\frac{x^s}{s}\right) = x,$$

$$\int_{c+iT}^{a+iT} \cdots ds = O\left(\frac{x}{T}\log^2(T)\right), \quad \int_{a-iT}^{c-iT} \cdots ds = O\left(\frac{x}{T}\log^2(T)\right), \qquad \leftarrow \text{mon. fallend in } T$$

und $$\int_{a-iT}^{a+iT} \left(-\frac{\zeta'}{\zeta}(s)\right)\cdot\frac{x^s}{s}\,ds = O\left(\frac{x\log^3(T)}{\exp\left(A_0\frac{\log(x)}{\log(T)}\right)}\right). \qquad \leftarrow \text{mon. wachsend in } T$$

Wähle T so, dass $\frac{x}{T} = \frac{x}{\exp\left(A_0\frac{\log(x)}{\log(T)}\right)}$, also für $\log T = \frac{\log(x)}{\log(T)} \Leftrightarrow \log(T) = \sqrt{\log(x)}$.

Es folgt $\psi(x) = x + O\left(\frac{x}{\exp(A_0\sqrt{\log(x)})}\right)$.

Die Bed. $x = m + \frac{1}{2}$ kann entfallen. $\square$

5.5 Kor. (PZS für π, 1. Version): Ex. $c_1 > 0$: $\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{\exp(c_1\sqrt{\log(x)})}\right)$.

Bew.: Aus der Version $\psi(x) = x + O\left(\frac{x}{\exp(c_0\sqrt{\log(x)})}\right)$ folgt die Version für ϑ, und π mittels partieller Σ und leichter Abänderung von c_0 in c_1:

Wegen $\psi(x) = \vartheta(x) + O(\sqrt{x})$ nach Bem. 2.9(b) folgt auch

$\vartheta(x) = x + O\left(\frac{x}{\exp(c_0\sqrt{\log x})}\right)$. Partielle Summation zeigt dann

$$\pi(x) = \sum_{p^k \le x} \log(p)\cdot\frac{1}{\log(p)} = \vartheta(x)\frac{1}{\log(x)} + \int_2^x \vartheta(t)\,\frac{dt}{t\log^2(t)}, \qquad R(t) := \vartheta(t) - t$$

$$= \frac{t}{\log t}\Big|_2^x - \int_2^x t\left(\frac{1}{\log t}\right)'dt + O\left(\frac{x}{\exp(c_0\sqrt{\log x})}\right) + \int_2^x R(t)\,\frac{dt}{t\log t}$$

$$\hookrightarrow R(t) \ll \frac{t}{\exp(c_0\sqrt{\log t})}$$

$$= \underbrace{\int_2^x \frac{dt}{\log t}}_{=\mathrm{li}(x)} + O\left(\frac{x}{\exp(c_1\sqrt{\log x})}\right) \quad \text{mit } c_1 = \sqrt{\tfrac{1}{2}}\cdot c_0.$$

$$\hookrightarrow \ll \underbrace{\int_2^{\sqrt{x}} \cdots}_{O(\sqrt{x})} + \int_{\sqrt{x}}^x \frac{t}{\exp(\underbrace{\sqrt{\tfrac{1}{2}}c_0}_{c_1}\sqrt{\log x})}\cdot\frac{dt}{t}$$

$\square$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a6: Explizite Formeln

Stichworte: explizite Formel für ψ, von-Mangoldt-explizite Formel, Restterme und Supremum der Nullstellenrealteile, Formulierungen der (RH)

6.1. Einleitung: Wir formulieren noch den PZS für ψ so, dass die Nullst. von ζ darin direkt auftreten. Eine derartige Formel nennt man explizite Formel.

6.2. Satz (explizite Formel für ψ):
Sei $x = m+\frac{1}{2}$ und $m \in \mathbb{N}$. Es bezeichne $\rho = \beta + i\gamma$ eine Nst. von ζ mit $0<\beta<1$. Dann ist für $x \geq 1$ und $1 \leq T \leq x$:

$$\psi(x) = x - \sum_{\rho, |\gamma| \leq T} \frac{x^\rho}{\rho} + O\left(\frac{x}{T}\log^2(x)\right).$$

Dabei kommen die Nst. in der Summe gemäß ihrer Vielfachheit vor.

Bew.: Verwenden wieder Lemma 4.2 aus der Perronschen Formel, ergänzen den Integrationsweg diesmal um ein Rechteck, das die Nst. von ζ umfasst. Nach Lemma 4.9 gilt für die Anz. der Nst. mit $|\gamma - T| \leq \frac{1}{2}$ die Absch. $N(T+\frac{1}{2}) - N(T-\frac{1}{2}) \ll \log(T)$.

[Es gibt also ein $c_0>0$ und $T' \in [T-\frac{1}{2}, T+\frac{1}{2}]$ mit $|\gamma - T'| \geq \frac{c_0}{\log(T')}$ für alle Nst. $\rho = \beta + i\gamma$ von ζ.
Die Ersetzung von $\sum_{\rho, |\gamma| \leq T} \frac{x^\rho}{\rho}$ durch $\sum_{\rho, |\gamma| \leq T'} \frac{x^\rho}{\rho}$ macht den Unterschied

$$\left| \sum_{\rho, |\gamma| \leq T} \frac{x^\rho}{\rho} - \sum_{\rho, |\gamma| \leq T'} \frac{x^\rho}{\rho} \right| \ll \frac{x}{T'} \cdot \log(T'),$$

es genügt also, die Beh. mit T' anstelle T zu zeigen, schreiben im folgenden wieder T für T'.]

Setzen also OE $|\gamma - T| \geq \frac{c_0}{\log(T)}$ (+) für alle Nst. ρ von ζ voraus.

Ergänze den Integrationsweg $[c-iT, c+iT]$ durch

$$\mathcal{C} = [c-iT, c+iT] \cup [c+iT, -\tfrac{1}{2}+iT] \cup [-\tfrac{1}{2}+iT, -\tfrac{1}{2}-iT] \cup [-\tfrac{1}{2}-iT, c-iT].$$

Für $s \in [c+iT, -\frac{1}{2}+iT]$ haben wir nach Lemma 4.9 und (+)

$$\frac{\zeta'}{\zeta}(s) = \sum_{|\beta-T|<1} \frac{1}{s-\rho} + O(\log(T)) = O((N(T+1)-N(T-1))\log(T)) + O(\log(T)) = O(\log^2(T)),$$

damit $\int_{c+iT}^{-1/2+iT} \dots, \int_{-1/2-iT}^{c-iT} \dots = O\left(\frac{x}{T}\log^2(T)\right)$.

Für $s = -1/2 + it$ mit $t \in [-T, T]$ ist nach Lemma 4.9

$$\frac{\zeta'}{\zeta}(s) = \sum_{|\gamma-t|<1} \frac{1}{s-\rho} + O(\log|t|), \text{ also } \int_{-1/2-iT}^{-1/2+iT} \dots = O(x^{-1/2}\log^2(T)).$$

Nach dem Residuensatz ist $\frac{1}{2\pi i}\int_{\mathcal{C}} \dots = \mathrm{Res}_1\left(-\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\right) + \sum_{\rho, |\gamma|\le T} \mathrm{Res}_\rho\left(-\frac{\zeta'}{\zeta}(s)\cdot\frac{x^s}{s}\right) + \mathrm{Res}_0\left(-\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\right)$

$$= x - \sum_{\rho, |\gamma|\le T} \frac{x^\rho}{\rho} + O(1). \qquad \square$$

6.3. Notation: • Für die nichttrivialen Nullstellen $\rho \in \mathbb{C}$ von ζ schreibt man $\rho = \beta + i\gamma$, wo also $0 < \beta < 1$, $\gamma \in \mathbb{R}$ (also $|\gamma| > 14$ laut numerischen Werten).

• Werden die Nullstellen mit $\gamma > 0$ durchnumeriert, schreibt man $\rho_n = \beta_n + i\gamma_n$, $n \in \mathbb{N}$.

Aus der Funktionentheorie ist bekannt, dass sich Nullstellen einer holomorphen Fkt. nirgendwo häufen.

6.4. Bem.: • Man vermutet, dass alle diese Nullstellen einfache Nullstellen sind, so dass in der Summe alle Summanden tatsächlich verschieden sind.

• Ohne O-Termen kann die explizite Formel auch gezeigt werden, eine Verfeinerung des Beweises von 6.2 gibt folgende Version:

6.5. Satz (die von-Mangoldt-explizite Formel):

Sei $\psi_0(x) := \frac{1}{2}\left(\sum_{n<x}\Lambda(n) + \sum_{n\le x}\Lambda(n)\right)$. [also ist $\psi_0(x) = \psi(x)$ für $x \notin \mathbb{Z}$]

Dann ist

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right) - \log(2\pi),$$

wo ρ genau die Nst. von ζ in $0<\sigma<1$ gemäß Vielfachheiten durchläuft.

[Bew.: s. [Davenport], Kap. 17]

Bem.: Wegen $-\frac{1}{2}\log\left(1-\frac{1}{x^2}\right) = \sum_{n\ge1}\frac{x^{-2n}}{2n} = -\sum_{n\ge1}\frac{x^{-2n}}{-2n}$, wo $\{-2n; n\in\mathbb{N}\}$ die trivialen Nst. von ζ durchläuft, kann diese explizite Formel in der Form $\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \log(2\pi)$ geschrieben werden, wo ρ alle Nst. von ζ durchläuft.

Wir gehen den Zusammenhängen zwischen Nullstellenfreiheit von ζ in $0<\sigma<1$ und PZS-Versionen mit Resttermabschätzung noch genauer auf den Grund.

6.6. **Def.:** Seien $A := \inf\{\alpha;\ \forall \varepsilon>0: \psi(x) = x + O_\varepsilon(x^{\alpha+\varepsilon})\}$,
und $B := \sup\{\beta;\ \exists\, \rho=\beta+i\gamma : \zeta(\rho)=0\}$.

6.7. **Bem.:** A ist also der kleinste Exponent ≤ 1 in der Resttermabschätzung für den PZS in der ψ-Version, und B das Supremum der Realteile der ζ-Nullstellen.

6.8. **Satz:** Es gilt $A=B$. Insbesondere gilt:
$$(RH) \Leftrightarrow \forall \varepsilon>0: \psi(x) = x + O_\varepsilon(x^{1/2+\varepsilon}) \Leftrightarrow \forall \varepsilon>0: \pi(x) = li(x) + O_\varepsilon(x^{\frac{1}{2}+\varepsilon}).$$

Bew.: • $A \le B$: Wende die explizite Formel 6.2 an mit $T=x$.

Für $x = m+\frac{1}{2}$, $m\in\mathbb{N}$, erhalten wir $\psi(x) = x - \sum_{|\gamma|\le x} \frac{x^\rho}{\rho} + O(\log^2(x))$.

Haben $\left|\sum_{|\gamma|\le x} \frac{x^\rho}{\rho}\right| \le 2x^B \left(\sum_{1\le\gamma\le x} \frac{1}{\gamma} + O(1)\right)$.

$\left[\sum_{|\gamma|\le 1} \frac{1}{|\rho|} = O(1)\right.$, nahe 0 liegen keine Nst. von ζ, da $\zeta(0) = -\frac{1}{2}$ & Stetigkeit$\left.\right]$

Wähle J mit $2^J \le x < 2^{J+1}$,
erhalten $\sum_{1\le\gamma\le x} \frac{1}{\gamma} \le \sum_{j=0}^{J} 2^{-j} \sum_{2^j\le\gamma\le 2^{j+1}} 1 = \sum_{j=0}^{J} 2^{-j}\left(N(2^{j+1}) - N(2^j)\right)$.

Haben $N(2^{j+1}) - N(2^j) = O(2^j \log 2^j) = O(j2^j)$ nach Lemma 4.9,
also $\sum_{1\le\gamma\le x} \frac{1}{\gamma} = \sum_{j=0}^{J} O(j) = O(J^2) = O(\log^2(x))$.

Somit folgt: $\psi(x) = x + O_\varepsilon(x^{B+\varepsilon})$ für alle $\varepsilon>0$, also $A\le B$.

• $B \le A$: Es gilt $\forall \varepsilon>0: \psi(x) = x + O_\varepsilon(x^{A+\varepsilon})$.

Für $\sigma>1$ setzen wir $F(s) = -\frac{1}{s}\cdot\frac{\zeta'}{\zeta}(s) - \frac{1}{s-1}$, $G(s) = \int_1^\infty (\psi(x)-x)x^{-s-1}\,dx$.

Eine partielle Summation (für $\sigma>1$) zeigt, dass
$$-\frac{\zeta'}{\zeta}(s) = \sum_{n\ge1} \Lambda(n) n^{-s} = s\int_1^\infty \psi(x) x^{-s-1}\,dx, \quad \text{vgl. Bew. 1.) in AnZ 15.2}$$
$a_n = \Lambda(n)$, $f(t) = t^{-s}$

also

$$F(s) = -\frac{1}{s}\cdot\frac{\zeta'}{\zeta}(s) - \frac{1}{s-1} = \int_1^\infty \underbrace{(\psi(x)-x)}_{\ll_\varepsilon x^{A+\varepsilon}} x^{-s-1}\,dx = G(s).$$

Somit ist die Folge $G_N(s) := \int_1^N (\psi(x)-x)\,x^{-s-1}\,dx$ in $\sigma > A$ kp. kgt. gegen $G(s)$.

Damit ist $G(s)$ holom. für $\sigma > A$, und $F(s)$ hat keinen Pol für $\sigma > A$.

Dies heißt $\zeta(s) \neq 0$ für $\sigma > A$, woraus $B \leq A$ folgt. □

6.9. Bem.: • Man betrachte auch $\tilde{A} := \inf\{\alpha;\ \forall \varepsilon > 0 : \pi(x) = li(x) + O_\varepsilon(x^{\alpha+\varepsilon})\}$.
Eine partielle Summation zeigt $\tilde{A} = A$. • Ob $A < 1$ bzw. $B < 1$, ist unbekannt.
• Nimmt man die (RH) an, kann für ψ bzw. π eine noch schärfere Asymptotik gezeigt werden:

6.10. Kor.: (RH) $\Rightarrow \psi(x) = x + O(x^{1/2}\log^2(x))$. $\left[\overset{\text{part. }\Sigma}{\Rightarrow} \pi(x) = li(x) + O(x^{1/2}\log(x))\right]$ vgl. 2.19

Bew.: Obiger Bew. in "$A \leq B$" zeigt $\sum_\rho \frac{x^\rho}{\rho} = O(x^B \log^2(x))$, also $\psi(x) = x + O(x^B \log^2(x))$.
Ist die (RH) wahr, gilt $B = \frac{1}{2}$, es folgt die Beh. □

6.11. Bem.: • Es gibt noch sehr viele andere Aussagen, die zur (RH) äquivalent sind. Für gewöhnlich kann man für die Implikationen "(RH) $\Rightarrow$ ..." dann Verschärfungen finden.
• Zur Sprechweise: Mathematische Aussagen, die unter der Ann. der (RH) gelten [manchmal auch unter Ann. anderer unbewiesener Vermutungen], heißen konditionell. Aussagen, die ohne Annahme unbewiesener Vermutungen (o.A.u.V.) gezeigt werden können, heißen unkonditionell.
• Es gibt noch weitere "explizite Formeln", etwa folgende:

6.12. Satz (Riemann-explizite Formel): Für $J(x) := \sum_{k \geq 1} \frac{1}{k}\pi(x^{1/k})$ gilt
$$J(x) = Li(x) - \sum_\rho Li(x^\rho) - \log(2) + \int_x^\infty \frac{dt}{t(t^2-1)\log(t)},$$ wo $Li(x) := \int_0^x \frac{dt}{\log(t)} = \lim_{\varepsilon \to 0+}\left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^x\right)\frac{dt}{\log(t)}$,
wo ρ über die nichttrivialen Nst. von ζ läuft.

[Bew.: [Edwards, §3.7]]

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a7: Weylsche Exponentialsummen

Stichworte: Weylsche Exponentialsumme, Weylsche Ungleichung, Vinogradov-Integral, Vinogradovs Mittelwertsatz, k-ter Ableitungstest, nullstellenfreies Gebiet / PZS (2. Version)

7.1. Einleitung: Wir skizzieren die Bausteine einer modernen Herangehensweise zum Beweis des Vinogradov-Korobov-nullstellenfreien Gebiets samt zugehörigem PZS (2. Version).

7.2. Def.: Eine allgemeine Weylsche Exponentialsumme bzw. trigonometrische Summe ist eine Summe der Form $\sum_{a<n\le x} e(f(n))$, $f:\mathbb{R}\to\mathbb{R}$, $e(t):=e^{2\pi i t}$.
Ist f eine Polynomfunktion, spricht man von einer Weylschen Exponentialsumme.

7.3 Bem.: • Eine der Ideen von Weyl besteht darin, f mit Taylors Satz durch Polynome zu entwickeln, und so das Studium der ursprünglichen Summe auf das der Summen mit Polynomen zurückzuführen. Das geht sehr gut mit $\sum_n n^{it} = \sum_n e(\frac{t}{2\pi}\log n)$ zum Studium der ζ-Fkt. (und des PZS) und führt uns auf Verbesserungen im Fehlerterm des PZS in einer 2. Version.

• Die Dirichletreihe $\sum_{n\ge 1} n^{-s}$ für $\zeta(s)$, $\sigma>1$, konvergiert zwar nicht mehr für $\sigma\le 1$. Dennoch können die Partialsummen zur Approximation herangezogen werden, und es gibt folgende Möglichkeiten dafür:

(1.) Hardy-Littlewood-Approximationsformel: $\zeta(s) = \sum_{n\le x} n^{-s} - \frac{x^{1-s}}{1-s} + O(x^{-\sigma})$, $|t|\le 4x$, $\sigma>0$.
(vgl. Satz 1.16)

(2.) Die approximative Funktionalglg.: $\zeta(s) = \sum_{n\le x} n^{-s} + \Delta(s)\sum_{n\le y} n^{s-1} + O((x^{-\sigma}+t^{\frac12-\sigma}y^{\sigma-1})\log(t))$,
$\Delta(s)=\frac{(2\pi)^s}{2\cos(\frac{\pi s}{2})\Gamma(s)}$, wo $2\pi xy = t$, $x\ge 1$, $y\ge 1$, $0<\sigma<1$.

Obere Schranken für $\sum_{n\le x} n^{\sigma+it} = \sum_{n\le x} n^{\sigma}\cdot e(\frac{t}{2\pi}\log(n))$ mit Weylsummen führen so auf ob. Schranken für $\zeta(s)$, mit Satz 9.1. auf nullstellenfreie Gebiete und dann auf den PZS.

7.4. Bem.: Offenbar hängt $e(f(n))$ nur vom gebrochenen Teil $f(n)-\lfloor f(n)\rfloor\in[0,1)$ ab.
Weylsche Exponentialsummen hängen eng mit der Theorie der Gleichverteilung von Folgen zusammen.

7.5. Sei $f \in \mathcal{C}^{a+1}(\mathbb{R},\mathbb{R})$. Die Approximation von f mit einem Taylorpolynom führt auf

$$\sum_{0<m\le x-a} e(f(a+m)) = \sum_{\nu=0}^{\infty} c_\nu \sum_{m=1}^{x-a} m^\nu e\left(f'(a)m + \dots + \frac{f^{(k)}(a)}{k!} m^k\right)$$

mit $c_\nu \in \mathbb{R}$. Ist $|c_\nu|$ hinr. klein, kann die Absch. dieser Exponentialsummen auf die von $\sum_{m\le N} e(P(m))$, $P(m) = P_k(m) = f'(a)m + \dots + \frac{f^{(k)}(a)}{k!} m^k$ zurückgeführt werden. Wir beschränken uns daher auf solche Weylsummen mit Polynomen.

Hierzu konnte Weyl die folgende Unglg. zeigen.

7.6. Satz (Weylsche Ungleichung): Es sei $P_k(x) = \alpha_k x^k + \dots + \alpha_0$ mit $\alpha_i \in \mathbb{R}$, $k \ge 1$, sowie $S = \sum_{n\le N} e(P_k(n))$. Der Leitkoeff. α_k sei gut durch eine rationale Zahl $\frac{a}{q}$ approximiert, nämlich so, dass $|\alpha_k - \frac{a}{q}| \le \frac{1}{q^2}$, wo $a \in \mathbb{Z}, q \in \mathbb{N}$. Es sei $K = 2^{k-1}$, $\varepsilon > 0$, dann ist

$$S \ll_{a,\varepsilon} \underbrace{N^{1+\varepsilon}}_{\text{triv. Abschätz.}} \underbrace{\left(N^{-1} + q^{-1} + N^{-k} q\right)^{1/K}}_{\text{Verbesserung, je kleiner } K \text{ desto besser.}}.$$

7.7. Mittlerweile ist diese Absch. überholt. Vinogradov selbst konnte für $N \le q \le N^{k-1}$ die Absch. $S \ll_k N^{1-1/(11k^2 \log k)}$ zeigen.

Vinogradov's Methode verwendet nichttriviale Absch. für das Vinogradov-Integral $J_{s,k}(N) = \int_{[0,1]^k} |S_N(\underline{\alpha})|^{2s} d\underline{\alpha}$, $S_N(\underline{\alpha}) = S$ wie oben.

Anders ausgedrückt, ist $J_{s,k}(N)$ die Anzahl der ganzzahligen Lösungen des Vinogradov-Systems

$$\left\{\begin{array}{l} m_1 + \dots + m_s = n_1 + \dots + n_s \\ m_1^2 + \dots + m_s^2 = n_1^2 + \dots + n_s^2 \\ \vdots \\ m_1^k + \dots + m_s^k = n_1^k + \dots + n_s^k \end{array}\right\}$$

mit $1 \le m_1, \dots, m_s, n_1, \dots, n_s \le N$,

welches auch in anderen Anwendungen in der Mathematik vorkommt. Die lange offene Vermutung zur oberen Schranke von $J_{s,k}(N)$ wurde erst kürzlich bestätigt.

7.8. Satz (Bourgain/Demeter/Guth, Wooley 2015): Für $s, k \in \mathbb{N}$, $x \in \mathbb{R}_{>1}$, ist $\forall \varepsilon > 0$:
("Vinogradovs Mittelwertsatz")

$$J_{s,k}(x) \ll_\varepsilon x^\varepsilon \left(x^s + x^{2s - k(k+1)/2}\right).$$

Der Beweis erfordert entweder umfangreichen Einsatz neuer Ergebnisse der Forschung zur harmonischen Analysis (Restriktionstheorie, [BDG]), oder umfangreiche Überlegungen mit einer Methode namens "effizienten Kongruenzen" nach [Wooley].

Es ist unmöglich, eine obere Schranke für S zu zeigen, die das Vinogradov-Integral $\mathcal{J}_{s,k}(N)$ beinhaltet:

7.9. Satz (Montgomery):

$$S \ll_{k,s} N \cdot \left(\frac{\mathcal{J}_{s,k-1}(3N)}{N^{2s-k(k-1)/2}}\right)^{\frac{1}{2s}} \cdot \left(\frac{1}{q} + \frac{\log(q)}{N} + \frac{q\log(q)}{N^k}\right)^{\frac{1}{2s}}.$$

[Bew.: s. Montgomery "Ten Lectures...", Thm. 4 in §4]

7.10. Kor. aus VMWS:

$$S \ll_k N^{1+\varepsilon}\left(\frac{1}{q} + \frac{\log(q)}{N} + \frac{q\log(q)}{N^k}\right)^{\frac{1}{k(k-1)}}.$$

[Beste bekannte Weylsche Ungl.g. $\rightsquigarrow k = \frac{1}{k(k-1)}$ in 7.6.]

Bew.: Verwende den "kritischen Exponenten" $s = k-1$ in VMWS und setze ein. □

7.11. Bem.: Der Exponent $K = 2^k$ konnte somit auf $k(k-1)$ gedrückt werden. Von Montgomerys Vermutung, dass im Kor. auf den Term $\frac{\log(q)}{N}$ verzichtet werden könnte, und sogar $\frac{1}{k(k-1)}$ zu $\frac{1}{k}$ verbessert bar sei, sind wir womöglich noch weit entfernt.

Ist die Größe der k-ten Ableitung von f bekannt, kann eine obere Schranke der Weylsumme $\sum_{n\le N} e(f(n))$ in Abhängigkeit dieser Größe gezeigt werden:

7.12. Satz (k-ter Ableitungstest, [Heath-Brown 2016] nach VMWS):
Sei $k \ge 3$, $f \in \mathcal{C}^k([0,N],\mathbb{R})$. Weiter sei $0 < \lambda \le |f^{(k)}(x)| \le A\lambda$ für $x \in (0,N)$.
Dann:

$$\sum_{n\le N} e(f(n)) \ll_{A,k,\varepsilon} N^{1+\varepsilon}\left(\lambda^{1/k(k-1)} + N^{-1/k(k-1)} + N^{-2/k(k-1)}\lambda^{-2/k^2(k-1)}\right).$$

Wir geben lediglich die Bausteine dieses Satzes an (ohne Beweis):

7.13. Lemma: Sei $k \ge 2$, f wie in 7.12, sei $A\lambda \le \frac{1}{4}$. Dann ist (für $s \in \mathbb{N}$):

$$\sum_{n\le N} e(f(n)) \ll H + k^2 N^{1-1/s} \mathcal{N}^{1/2s} \cdot \left(H^{-2s+k(k-1)/2}\, \mathcal{J}_{s,k-1}(H)\right)^{1/2s}$$

mit $H = \lfloor (A\lambda)^{-1/k} \rfloor$ und $\mathcal{N} := \#\left\{m,n \le N;\ \left\|\frac{f^{(j)}(m)}{j!} - \frac{f^{(j)}(n)}{j!}\right\| \le 2H^{-j},\ 1 \le j \le k-1\right\}$.

Dabei ist $\mathcal{J}_{s,k-1}(H)$ das Vinogradov-Integral. [Bew.: Taylorapprox. von f, Weylsummen mit Polynomen wie in Satz 7.9 von Montgomery.]

Weiter besteht die Neuerung von [Heath-Brown] darin, $\mathcal{N}$ besser als wie bislang bekannt war, abzuschätzen:

7.14. **Lemma:** Für $k \geq 3$, f wie in 7.12, $A\lambda \leq \frac{1}{4}$, ist $\mathcal{N} \ll ((k-1)!\,A)^4 \,(N + \lambda N^2 + \lambda^{-2/k}) \log(N)$

Beweis von Satz 7.12:

Setzen wir Lemma 7.14 ein in Lemma 7.13 und verwenden VMVS Satz 7.8 in der Form $\mathcal{J}_{s,k-1}(H) \ll H^{2s-k(k-1)/2+\varepsilon} \underset{s=k(k-1)/2}{=} H^{k(k-1)/2+\varepsilon}$,

so erhalten wir

$$\sum_{n\leq N} e(f(n)) \ll N^{\varepsilon}\Big(\underbrace{\lambda^{-1/k}}_{\text{kann entfallen}} + N^{1-1/k(k-1)} + N\lambda^{1/k(k-1)} + N^{1-2/k(k-1)}\lambda^{-2/k^2(k-1)}\Big).$$

nach etwas Überlegung: die anderen Summanden dominieren

□

Dies ergibt die zur Zeit beste bekannte Absch. von ζ im kritischen Streifen:

7.15. **Satz (Heath-Brown):** Sei $\kappa = \frac{8}{63}\sqrt{15} = 0.4918\ldots$

Für $\varepsilon > 0$ ist dann $\zeta(\sigma + it) \ll_\varepsilon t^{\kappa(1-\sigma)^{3/2}+\varepsilon}$, glm. in $t \geq 1$, $\frac{1}{2} \leq \sigma \leq 1$.

⌜Ehemaliger Rekord von K. Ford 2002 war 4.45 für κ.⌟

Bew.: Satz 7.12 wird angewendet auf $f(n) = \frac{-t}{2\pi}\log n$

da $n^{-it} = e^{-it\log n} = e\left(\frac{-t}{2\pi}\log n\right)$ gilt. Dieser Satz liefert nun neue Abschätzungen für $\sum_{n\leq N} e(f(n)) = \sum_{n\leq N} n^{-it}$ in Abh. von $\lambda = \frac{t}{2\pi}\cdot(k-1)!\cdot N^{-k}$.

Diese lässt sich weiterbehandeln im Sinne der sogenannten "Exponentenpaartheorie" $\rightsquigarrow \sum_{n\in I} n^{-it} \ll_\varepsilon N^{1-49/80\tau^2+\varepsilon}$, $\tau = \frac{\log t}{\log N} \geq 2$, I bel. Teilintervall von $(N, 2N]$. } ohne Details hier

Part. $\sum \rightsquigarrow \sum_{n\in I} n^{-\sigma-it} \ll N^{-\sigma+1-49/80\tau^2+\varepsilon} \leq t^{(1-\sigma)\tau^{-1} - \frac{49}{80}\tau^{-3}+\varepsilon}$ für $\frac{1}{2} \leq \sigma \leq 1$. ⌜$N = t^{\tau^{-1}}$⌟

Die Wahl $\tau = \sqrt{\frac{147}{80}\cdot\frac{1}{1-\sigma}}$ zeigt $\sum_{n\in I} n^{-\sigma-it} \ll t^{\kappa(1-\sigma)^{3/2}+\varepsilon}$. Nun kann die Bed. $I \subseteq (N, 2N]$ entfallen mit einer Zusatzüberlegung.

Die Anwendung der approximativen Funktional-Glg., Bem. 7.3.(2), liefert damit auch $\zeta(s) \ll t^{\kappa(1-\sigma)^{3/2}+\varepsilon}$. □

Erhalten so ein verbessertes nullstellenfreies Gebiet:

7.16. **Satz** (nullstellenfreies Gebiet, 2. Version):
Es ist $\zeta(s) \neq 0$ für $t \geq 0$ und $\sigma \geq 1 - \frac{c_0}{(\log t)^{2/3} (\log\log t)^{1/3}}$ für ein $c_0 > 0$.
Dort ist $\frac{\zeta'}{\zeta}(s) \ll (\log t)^{5/3} (\log\log t)^{1/3}$.

Bew.:
Für $\sigma \geq 1 - A_0 \left(\frac{\log\log t}{\log t}\right)^{2/3} =: 1 - \theta(t)$ für ein $A_0 > 0$, nach Satz 7.15 haben wir

$$\zeta(s) \ll t^{\kappa A_0^{\frac{3}{2}} \frac{\log\log t}{\log t}} = e^{\kappa A_0^{3/2} \log\log t} =: e^{\Phi(t)}.$$

(Vernachlässigen ε $\rightsquigarrow$ κ größer)

Wenden nun den allgemeinen Satz 5.2 zum nullstellenfreien Gebiet von ζ an mit $\Phi(t) = \kappa A_0^{3/2} \log\log t$, $\theta(t) = A_0 \left(\frac{\log\log t}{\log t}\right)^{2/3}$.
Dieses liefert, dass $\zeta(s) \neq 0$ für $\sigma > 1 - c_0 \cdot \frac{\left(\frac{\log\log t}{\log t}\right)^{2/3}}{\log\log t} = 1 - \frac{c_0}{(\log t)^{2/3} (\log\log t)^{1/3}}$. ✓
Die Konstante $c_0 > 0$ hängt von κ, A_0 ab (und ist numerisch berechenbar, noch durch geschickte Wahl von A_0).
Dieser zeigt ferner, dass $\frac{\zeta'}{\zeta}(s) \ll \frac{\log\log t}{\left(\frac{\log\log t}{\log t}\right)^{2/3}} \cdot \log t = (\log t)^{5/3} (\log\log t)^{1/3}$. ✓

□

7.17. **Bem.:** Das in Satz 7.16. nachgewiesene nullstellenfreie Gebiet

$$\sigma \geq 1 - \frac{c_0}{(\log t)^{2/3} (\log\log t)^{1/3}}$$

wurde bereits von [Korobov & Vinogradov, 1958] gezeigt und konnte bis heute nicht wesentlich verbessert werden.
Der Einfachheit halber haben wir uns nicht um den numerischen Wert der Konstanten c_0 gekümmert.
[K. Ford] zeigte 2002, dass $c_0 = \frac{1}{57.54}$ genommen werden kann.

Die Verwendung des vor Kurzem bewiesenen VMWS um neue effektive Verbesserungen der implizite Konstanten darin führen bislang lediglich zu neuen Verbesserungen in der Konstanten c_0.

Wir zeigen noch, wie die zur Zeit beste Version des PZSes (von Korobov/Vinogradov) jetzt hergeleitet werden kann.

7.18 Satz (PZS mit Fehlerterm, 2. Version):

Es gibt $A_0, \tilde{A}_0 > 0$ mit $\psi(x) = x + O\left(x \exp\left(-A_0 (\log x)^{3/5} (\log\log x)^{-\frac{1}{5}}\right)\right)$

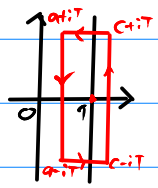
und $\pi(x) = \mathrm{li}(x) + O\left(x \exp\left(-\tilde{A}_0 (\log x)^{3/5} (\log\log x)^{-1/5}\right)\right)$.

Bew.: 1.) Zeige die Formel für ψ:

Dazu sei $T = T(x) > 1$, $c = c(x) = 1 + \frac{1}{\log x}$, $x = m + \frac{1}{2}$ mit $m \in \mathbb{N}$.

Nach Lemma 4.2 (aus der Perron'schen Formel)

haben wir $\psi(x) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds + O\left(\frac{x}{T} \log^2(x)\right)$.



Ergänzen den Weg $[c-iT, c+iT]$ zur geschlossenen Kurve

$\mathcal{C} = [c-iT, c+iT] \cup [c+iT, a+iT] \cup [a+iT, a-iT] \cup [a-iT, c-iT]$,

wo $a = 1 - A_0 \left(\frac{\log\log T}{\log T}\right)^{2/3}$, und $A_0 > 0$.

Nach dem Residuensatz ist $\frac{1}{2\pi i} \int_{\mathcal{C}} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds = \mathrm{Res}_{s=1}\left(-\frac{\zeta'}{\zeta}(s) \cdot \frac{x^s}{s}\right) = x$. ✓

Nach Satz 7.16 ist $\frac{\zeta'}{\zeta}(s) \ll (\log t)^{5/3} (\log\log t)^{1/3}$.

Es folgen die Abschätzungen:

- horizontal:

$$\left(\int_{a-iT}^{c-iT} + \int_{c+iT}^{a+iT}\right) \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds = O\left(\frac{x}{T} \cdot (\log T)^{5/3} (\log\log T)^{1/3}\right),$$

$\ulcorner x^c = x \cdot e \ll x \lrcorner$

mon. ↓ in T,

sowie

- vertikal: $\int_{a-iT}^{a+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds = O\left(x \exp\left(-A_0 (\log x) \left(\frac{\log\log T}{\log T}\right)^{2/3}\right) \cdot \underbrace{(\log T)^{\frac{8}{3}} (\log\log T)^{\frac{1}{3}}}_{\text{Extra-}\log T \text{ von } \int_{-T}^{T} \frac{1}{|a+ti|} dt}\right)$

mon. ↑ in T.

Wähle T optimal so, dass $\underbrace{\frac{x}{T}}_{x \exp(-\log T)} \overset{!}{=} x \exp\left(-A_0 (\log x) \cdot \left(\frac{\log\log T}{\log T}\right)^{2/3} \cdot (\log\log T)^{-1}\right)$

d.h. $T = T(x)$ ist eine Fkt. mit $(\log T)^{\frac{5}{3}} \overset{!}{=} (\log x) (\log\log T)^{-1/3}$,

$\rightsquigarrow$ wähle: $\log T := (\log x)^{3/5} (\log\log x)^{-1/5}$

Erhalten so den Fehlerterm $O\left(x \exp\left(-A_0 (\log x)^{3/5} (\log\log x)^{-1/5}\right)\right)$.

2.) Zeige die Formel für π: Wegen $\vartheta(x) = \psi(x) + O(\sqrt{x} \log(x))$, vgl. Bem. 2.9 b),

folgt dieselbe Formel zunächst auch für $\vartheta(x)$. Dann partielle Σ

genau wie in Kor. 5.5 durchführen und die Konstante A_0

anpassen, dann folgt die behauptete Formel für π. □

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a8: Dirichletsche L-Reihen

Stichworte: Dirichlet-Charaktere, Dirichlet-L-Reihen, Eulerprodukt-Darstellung, merom. Fortsetzung, PZen in APen, Satz von Dirichlet, Funktionalgleichung von $L(s,\chi)$

8.1. Einleitung:
Das Studium der Primzahlen in arithmetischen Progressionen (APs) bzw. in Restklassen (d.h. $p \equiv a \bmod q$) ist eng mit der Theorie der Dirichletschen L-Reihen verbunden. Vorbild ist der Zusammenhang zwischen $\psi(x)$ und $\zeta(s)$, der auf $\psi(x;q,a)$ und den zugehörigen Dirichletreihen $L(s,\chi)$ verallgemeinert werden soll.
Die Koeffizientenfolgen heißen Dirichletcharaktere und sollen als erstes behandelt werden.

8.2. Def.: Sei $q \in \mathbb{N}$ und χ ein Charakter der Gruppe $(\mathbb{Z}/q\mathbb{Z},\cdot)^*$,
d.h. $\tilde{\chi}: (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$ sei Gruppenhomomorphismus $\lceil \tilde{\chi}(mn) = \tilde{\chi}(m)\tilde{\chi}(n) \rfloor$.
Die durch Forts. von $\tilde{\chi}$ auf $\mathbb{N}$ entstehende vollst. mult. zth. Fkt. $\chi: \mathbb{N} \to \mathbb{C}$, mit $\chi(n) = \tilde{\chi}(n \bmod q)$ falls $ggT(n,q)=1$ und $\chi(n)=0$ sonst, heißt Dirichletcharakter mod q. Ist $\tilde{\chi}$ der triviale Charakter von $(\mathbb{Z}/q\mathbb{Z},\cdot)^*$, so heißt χ der Hauptcharakter mod q und wird mit χ_0 bezeichnet.
$\lceil \rightsquigarrow \chi_0(n) = 1$ für $(n,q)=1 \rfloor$

8.3. Satz: Es gibt $\varphi(q)$ viele Dirichletcharaktere χ mod q, wobei φ die Eulersche φ-Fkt. ist (d.h. $\varphi(q) := \#\{0 < a \le q;\ ggT(a,q)=1\}$).

Bem.: $q=1 \Rightarrow \chi = \mathbb{1}$. Haben ja $\varphi(1)=1$.
Behandeln im folgenden nur noch D-Charaktere, schreiben dafür Charakter.

Bew.: • Für $m \in (\mathbb{Z}/q\mathbb{Z})^*$ und ein χ mod q ist $\chi(m)$ eine $\varphi(q)$-te EW. $\rightsquigarrow$ es ex. nur endlich viele Charaktere mod q.

• $\sum_{\chi(q)} \sum_{m(q)} \chi(m) = \sum_{m(q)} \chi_0(m) + \sum_{\chi \neq \chi_0} \sum_{m(q)} \chi(m) \underset{\substack{\text{ONR}\\ 8.4.a)}}{=} \sum_{m(q)} \chi_0(m) = \varphi(q)$.

• $\sum_{\chi(q)} \sum_{m(q)} \chi(m) = \sum_{\chi(q)} \chi(1) + \sum_{\chi(q)} \sum_{m \not\equiv 1(q)} \chi(m) \underset{\substack{\text{ONR}\\ 8.4.b)}}{=} \sum_{\chi(q)} 1$. Also: $\sum_{\chi(q)} 1 = \varphi(q)$. $\square$

8.4. Satz (Orthogonalitätsrelationen):

(a) ONR 1. Art: $\sum_{n \bmod q} \chi(n) = \varphi(q)$, falls $\chi = \chi_0$ und $= 0$ sonst,

und $\sum_{n \bmod q} \chi_1(n)\overline{\chi_2(n)} = \varphi(q)$ falls $\chi_1 = \chi_2$ und $=0$ sonst.

(b) ONR 2. Art: $\sum_{\chi \bmod q} \chi(n) = \varphi(q)$ falls $n \equiv 1 \bmod q$ und $=0$ sonst,

und $\sum_{\chi \bmod q} \chi(n_1)\overline{\chi(n_2)} = \varphi(q)$ falls $n_1 \equiv n_2 \bmod q$ und $=0$ sonst.

Bew.:

- Der 2. Teil der Aussage folgt mit $\chi = \chi_1\overline{\chi_2}$ bzw. $n_1 n_2^{-1}$ aus dem 1. Teil.
- (a): $\chi = \chi_0$ klar, $\chi \neq \chi_0$: Betr. m mit $\chi(m) \neq 1$. Dann: $\sum_{n(q)} \chi(n) = \sum_{n(q)} \chi(mn) = \chi(m)\sum_{n(q)} \chi(n) \Rightarrow \sum_{n(q)} \chi(n) = 0$.
- (b): $n \equiv 1 (q)$ klar, $n \not\equiv 1 (q)$: Betr. χ_1 mit $\chi_1(n) \neq 1$. Dann: $\sum_{\chi(q)} \chi(n) = \sum_{\chi(q)} (\chi\chi_1)(n) = \chi_1(n)\sum_{\chi(q)} \chi(n) \Rightarrow \sum_{\chi(q)} \chi(n) = 0$.

$\square$

8.5. Def.: Es sei $q \in \mathbb{N}$ und χ ein Charakter mod q. Unter der Dirichletschen L-Reihe $L(s,\chi)$ zu χ versteht man $L(s,\chi) = \sum_{n \geq 1} \chi(n) n^{-s}$, $\sigma > 1$.

8.6. Satz: Es sei $q \in \mathbb{N}$ und χ ein Charakter mod q. Dann ist $L(s,\chi)$ für $\sigma > 1$ normal konvergent (glm. kgt. auf Kompakta), und für $\chi \neq \chi_0$ sogar für $\sigma > 0$.
Somit stellt $L(s,\chi)$ für $\sigma > 1$ (bzw. für $\sigma > 0$ falls $\chi \neq \chi_0$) eine hol. Fkt. dar.
Für $\sigma > 1$ gilt die Eulerproduktdarstellung $L(s,\chi_0) = \zeta(s) \cdot \prod_{p \mid q} (1 - p^{-s})$, mit der $L(s,\chi_0)$ zu einer in $\sigma > 0$ meromorphen Fkt. fortgesetzt wird.

Bew.: Part. Σ zeigt $\sum_{n \geq 1} \chi(n) n^{-s} = \lim_{N \to \infty} \left(N^{-s} \cdot \sum_{n \leq N} \chi(n) \right) + s \int_1^\infty \underbrace{\left(\sum_{n \leq u} \chi(n)\right)}_{\text{beschränkt für } \chi \neq \chi_0} u^{-s-1} du$.

normale kgz. für $\sigma > 0$, bei $\chi = \chi_0$ für $\sigma > 1$.

Haben weiter $\chi_0(p) = \begin{cases} 0, & p \mid q \\ 1, & p \nmid q \end{cases}$,
also gilt für $\sigma > 1$:

$$L(s,\chi_0) \underset{\text{Euler-}\Pi\text{-Satz (Anf 8)}}{=} \prod_{p \nmid q} (1 - p^{-s})^{-1} = \prod_p (1 - p^{-s})^{-1} \prod_{p \mid q} (1 - p^{-s}) = \zeta(s) \prod_{p \mid q} (1 - p^{-s}). \quad \square$$

Der Zusammenhang zwischen $\psi(x;q,a)$ und $L(s,\chi)$ wird mit folgendem allg. Prinzip klar, das aus den ONR folgt.

8.7. Satz: Für eine zth. Fkt. f und $(a,q)=1$ ist für $x \geq 1$:

$$\sum_{\substack{n \leq x \\ n \equiv a(q)}} f(n) = \frac{1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a) \sum_{n \leq x} \chi(n) f(n),$$ wobei $\sum_{n \leq x}$ auch durch $\sum_{n=1}^{\infty}$ ersetzt werden kann, falls $\sum_n |f(n)|$ kgt.

Bew.: r.S. $= \sum_{n \leq x} f(n) \cdot \frac{1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a)\chi(n) = \sum_{n \leq x} f(n) \cdot \underbrace{\frac{1}{\varphi(q)} \sum_{\chi(q)} \chi(a^{-1}n)}_{\text{ONR: } =1 \text{ falls } a^{-1}n \equiv 1(q),\ =0 \text{ sonst}}$

$$= \sum_{\substack{n \leq x \\ n \equiv a(q)}} f(n).$$ □

Sei $(a,q)=1$. Die zu Pzen $p \equiv a(q)$ gehörige 2. Tsch.-Fkt. $\psi(x;q,a)$ und dazu gehörige erzeugende Dirichletreihe kann so mit den zugehörigen erzeugenden L-Reihen der Charaktere mod χ gewonnen werden:

8.8. Kor.: Es sei $q \in \mathbb{N}$, $(a,q)=1$, $\sigma > 1$. Dann ist

$$\sum_{n \equiv a(q)} \Lambda(n) n^{-\sigma} = \frac{1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a) \underbrace{\sum_{n \geq 1} \chi(n) \Lambda(n) n^{-\sigma}}_{= -\frac{L'}{L}(\sigma,\chi) \leftarrow \text{wie bei S}} = \frac{-1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a) \cdot \frac{L'}{L}(\sigma,\chi).$$ □

Ziel ist es nun, den Satz von Dirichlet zu beweisen. Mit 8.10.–8.15.

8.9. Satz (von Dirichlet): Sei $q \in \mathbb{N}$ und $ggT(a,q)=1$. Dann enthält die AP a mod q unendl. viele Pzen, d.h. $\#\{p \equiv a(q);\ p \in \mathbb{P}\} = \infty$.

(Insbesondere existiert stets mindestens eine Pz $p \equiv a(q)$.)

8.10. Satz: Sei $q \in \mathbb{N}$, χ ein Charakter mod q und $m_\chi \in \mathbb{N}_0$ die Vielf. der Nst. 1 von $L(\sigma,\chi)$, sei $(a,q)=1$.

Dann: $$\lim_{\sigma \to 1+} (\sigma-1) \sum_{n \equiv a(q)} \Lambda(n) n^{-\sigma} = \frac{1}{\varphi(q)} \Big(1 - \sum_{\chi \neq \chi_0} \overline{\chi}(a) \cdot m_\chi\Big).$$

Bew.: Verwenden, dass $L(s,\chi)$ für $\chi \neq \chi_0$ und $L(s,\chi_0) - \frac{1}{\sigma-1}$ Taylorentwicklungen in $\sigma_0 = 1$ (folgt mit Holomorphie der Fktn. aus Satz 8.6.) haben.

Betr. Kor. 8.8. für $\sigma > 1$, unter Verwendung von $L(s,\chi) \neq 0 \Rightarrow \frac{L'}{L}(\sigma,\chi) = O(1)$ für $\sigma \to 1+$.

Es habe $L(\sigma,\chi)$ eine Nst. der Vielf. m_χ in $\sigma = 1$. Haben dann die Taylorentwicklungen

$L(\sigma,\chi) = c_{m_\chi} (\sigma-1)^{m_\chi} + c_{m_\chi+1} (\sigma-1)^{m_\chi+1} + \ldots$ und

$L'(\sigma,\chi) = m_\chi c_{m_\chi} (\sigma-1)^{m_\chi-1} + \ldots$ um $\sigma_0 = 1$ mit $c_{m_\chi} \neq 0$.

Also: $\lim_{\sigma \to 1+} -(\sigma-1) \cdot \frac{L'}{L}(\sigma,\chi) = -m_\chi$. Weiter $\lim_{\sigma \to 1+} -(\sigma-1) \cdot \frac{L'}{L}(\sigma,\chi_0) = 1$.

Es folgt die Beh. mit Kor. 8.8. □

(auch: quadratisch, weil dann $\chi^2 = \chi_0$ gilt)

8.11. **Def.:** Der Char. χ mod q heißt **reell**, falls $\chi: \mathbb{N} \to \mathbb{R}$, andernfalls **komplex**.

8.12. **Satz:** (a) Für höchstens ein χ mod q ist $L(1,\chi) = 0$.

(b) Für komplexes χ ist $L(1,\chi) \neq 0$.

Bew.: (a): Folgt aus 8.10, da $\lim_{\sigma \to 1+} (\sigma - 1) \sum_{m \equiv 1 (q)} \Lambda(m) m^{-\sigma} \geq 0$. (Beachte: $a = 1 \sim \bar{\chi}(a) = 1$)

(b): Aus $L(1,\chi) = 0$ folgt $L(1,\bar{\chi}) = 0$. Für komplexe χ ist $\chi \neq \bar{\chi}$, und (b) folgt aus (a). □

8.13. **Satz:** Sei $\chi \neq \chi_0$ reell. Dann ist $\left| L(1,\chi) - \sum_{n \leq x} \chi(n) n^{-1} \right| = O_q(x^{-1})$

und $\left| L(\tfrac{1}{2},\chi) - \sum_{n \leq x} \chi(n) n^{-1/2} \right| = O_q(x^{-1/2})$.

Bew.: Für $\sigma > 0$ zeigt part. Σ: $\left| L(\sigma,\chi) - \sum_{n \leq x} \chi(n) n^{-\sigma} \right| = \sigma \cdot \int_x^\infty \left(\sum_{x < n \leq t} \chi(n) \right) t^{-\sigma-1} dt = O_q(x^{-\sigma})$. □

8.14. **Satz:** Für $\chi \neq \chi_0$ reell ist $L(1,\chi) \neq 0$.

Bew.: Sei $F(n) := \sum_{d|n} \chi(d) = \chi * \mathbb{1}(n)$, ist mult.

Für die Werte von F auf Primpotenzen gilt $F(p^\nu) = \sum_{0 \leq \lambda \leq \nu} \chi(p^\lambda) = \begin{cases} 1, & p \nmid q \\ \nu+1, & \chi(p) = 1 \\ 0, & \chi(p) = -1,\ 2 \nmid \nu \\ 1, & \chi(p) = -1,\ 2 \mid \nu \end{cases}$

Haben $F(p^\nu) \geq 0$ und $F(p^{2\nu}) \geq 1$,

also ist $F(n) \geq 0$ und $F(n^2) \geq 1$. Setze $G(x) = \sum_{n \leq x} F(n) n^{-1/2}$.

Es folgt $G(x) \geq \sum_{n \leq \sqrt{x}} F(n^2) n^{-1} \geq \sum_{n \leq \sqrt{x}} n^{-1} > \frac{1}{2} \log(x)$.

Andererseits ist

$$G(x) = \sum_{n \leq x} n^{-1/2} \sum_{d|n} \chi(d) = \sum_{d \leq \sqrt{x}} \chi(d) d^{-1/2} \sum_{t \leq x/d} t^{-1/2} + \sum_{t \leq \sqrt{x}} t^{-1/2} \sum_{\sqrt{x} < d \leq x/t} \chi(d) d^{-1/2}.$$

Nach der Eulerschen Summenformel 1.6. ist für $\sigma > 0$

$$\sum_{n \leq y} n^{-\sigma} = \int_1^y t^{-\sigma} dt - \sigma \underbrace{\int_1^y P_0(u) u^{-\sigma-1} du}_{= \int_1^\infty \ldots + O_\sigma(y^{-\sigma})} - y^{-\sigma} P_0(y) + P_0(1).$$

Mit $C_\sigma > 0$ passend folgt $\sum_{n \leq y} n^{-\sigma} = (1-\sigma)^{-1} y^{-\sigma+1} + C_\sigma + O_\sigma(y^{-\sigma})$.

Also ist $G(x) = \sum_{d \leq \sqrt{x}} \chi(d) d^{-1/2} \cdot \left(2 (x/d)^{1/2} + C_{1/2} + O((d/x)^{1/2}) \right) + \sum_{t \leq \sqrt{x}} \left(t^{-1/2} \cdot O(x^{-1/4}) \right)$

$(\sigma = \frac{1}{2})$ $\qquad (t/x)^{1/2} \ll x^{-1/4}$

$$= 2x^{1/2} \underbrace{\sum_{d \leq \sqrt{x}} \chi(d) d^{-1}}_{= L(1,\chi) + O(x^{-1/2})} + C_{1/2} \underbrace{\sum_{d \leq \sqrt{x}} \chi(d) d^{-1/2}}_{= L(\frac{1}{2},\chi) + O(x^{-1/4})} + O(1) \quad \leftarrow \text{nach } 5.12.$$

$$= 2x^{\frac{1}{2}} L(1,\chi) + O(1).$$

Aus $L(1,\chi) = 0$ würde $G(x) = O(1)$ folgen, im $\lightning$ zu $G(x) > \frac{1}{2} \log(x)$. □

8.15. **Kor.:** Sei $q \in \mathbb{N}$, $ggT(a,q)=1$. Dann: $\lim\limits_{\sigma \to 1^+} (\sigma-1) \cdot \sum\limits_{n \equiv a(q)} \Lambda(n) n^{-\sigma} = \frac{1}{\varphi(q)}$.

Bew.: Die Sätze 8.12 und 8.14 implizieren $m_\chi = 0$ für alle $\chi \neq \chi_0$ in Satz 8.10. (bel. a) $\square$

8.16. **Bew. des Satzes 8.9 von Dirichlet:**

Haben

$$\sum_{n \equiv a(q)} \Lambda(n) n^{-\sigma} = \sum_{p \equiv a(q)} (\log p) \cdot p^{-\sigma} + O(1) \text{ für } \sigma \to 1+,$$

denn $$0 \leq \sum_{p \equiv a(q)} \log p \sum_{k \geq 2} p^{-k\sigma} = \sum_p (\log p)\, p^{-2\sigma} \cdot \frac{1}{1-p^{-\sigma}} \overset{\sigma > 1}{\leq} \sum_p \frac{\log p}{p(p-1)} = O(1).$$

Aus Kor. 8.15. folgt somit, dass auch $\lim\limits_{\sigma \to 1+} \overbrace{(\sigma-1)}^{\to 0} \cdot \sum\limits_{p \equiv a(q)} (\log p) \cdot p^{-\sigma} = \frac{1}{\varphi(q)}$.
Also divergiert die Reihe, und $\#\{p \in \mathbb{P};\, p \equiv a(q)\} = \infty$. $\square$

8.17. **Bem.:** Auch für L-Reihen kann eine Funktionalglg. wie für ζ hergeleitet werden. Sie lautet ($q > 1$, χ primitiv, d.h. ohne Periode $< q$ ($\Rightarrow \chi \neq \chi_0$))

$$\Lambda(s,\chi) = \varepsilon(\chi) \cdot \Lambda(1-s, \bar{\chi}),$$

mit der vollständigen L-Reihe

$$\Lambda(s,\chi) = \left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\kappa}{2}\right) L(s,\chi),$$

$$\kappa = \tfrac{1}{2}(1-\chi(-1)), \quad \varepsilon(\chi) = i^{-\kappa} \cdot \frac{\tau(\chi)}{\sqrt{q}},$$

und der Gaußsumme $\tau(\chi) = \sum\limits_{m(q)} \chi(m) e^{2\pi i m/q}$.

$L(s,\chi)$ wird damit zu einer ganzen Fkt. fortgesetzt (d.h. holomorph auf $\mathbb{C}$).

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a9: Primzahlen in Progressionen

Stichworte: Primzahlsatz in Progressionen mit (vom Modul q abhängigem) Restglied, primitive Charaktere, Führungszahl, Eulerprodukt von $L(s,\chi)$

9.1. Einleitung:

Seien $a,q \in \mathbb{N}$ teilerfremd. Wir behandeln die Zählfunktionen der $p \equiv a\,(q)$.
Der Beweis des PZSes mit Restglied lässt sich auf PZen in Progressionen übertragen: Wegen $\psi(x;q,a) = \sum_{\substack{n\le x\\ n\equiv a\,(q)}} \Lambda(n) = \frac{1}{\varphi(q)} \sum_{\chi(q)} \bar\chi(a) \sum_{n\le x} \Lambda(n)\chi(n)$, vgl. 8.7,
kommt es auf die Koeff. von
$-\frac{L'}{L}(s,\chi) = \sum_{n\ge 1} \frac{\Lambda(n)}{n^s}\chi(n)$ an. Wieder wird die Perronsche Formel 3.12 angewendet,
sowie $L(1+it,\chi)\neq 0$ für $t>0$, $\chi^2 \neq \chi_0$.

Man erhält so ohne Probleme den PZS in Progressionen in der Form:

$$\psi(x;q,a) = \frac{x}{\varphi(q)}\left(1+o_q(1)\right), \quad \text{glm. für alle } a \text{ mit } (a,q)=1, \text{ wo } q \text{ fest.}$$

Eine partielle Σ liefert daraus wiederum die Version

$$\pi(x;q,a) = \frac{\mathrm{li}(x)}{\varphi(q)}\left(1+o_q(1)\right), \quad \text{glm. für alle } a \text{ mit } (a,q)=1, \text{ wo } q \text{ fest.}$$

Demnach sind die PZen auf den Restklassen $a \bmod q$, $(a,q)=1$, gleichverteilt: Pro Restklasse beträgt ihr (asymptotischer) Anteil $\frac{1}{\varphi(q)}$.

⌜Bsp.: Für $q=10$: $25\% = \frac{1}{4} = \frac{1}{\varphi(10)}$ aller PZen haben die Endziffer 1 (bzw. 3, 7 oder 9)⌟

Strebt man eine Version mit expliziter Fehlertermabschätzung an, so kann auf diesem Wege analog auch gezeigt werden, dass gilt:

9.2. PZS in arithmetischen Progressionen: Für $q\in\mathbb{N}$ und $x\to\infty$ gilt:

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O_q\left(\frac{x}{\exp(c_0\sqrt{\log x})}\right), \quad \text{alle } a \text{ mit } (a,q)=1,$$

$$\pi(x;q,a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \quad '' \qquad '' \qquad , \quad c_0 = c_0(q).$$

(d.h. der PZS mit Restterm, Satz 5.4, überträgt sich).

Bem.:
- Dies geht auch mit dem Vinogradov-Korobov-Fehlerterm, Satz 7.18
- Zeigen später mit dem Satz von Siegel-Walfisz 11.6 ein stärkeres Ergebnis.

In manchen Anwendungen des PZSes in Progressionen (z.B. Goldbachproblem) ist hingegen die Abhängigkeit des Fehlerterms von q wesentlich, oft kommt es auf die Gleichmäßigkeit des Satzes in einem weiten q-Bereich an. Ohne Ann. unbewiesener Vermutungen (unkonditionell) fällt der q-Bereich aber sehr klein aus, was wir hier behandeln möchten.

Wir benötigen zuerst noch einen Begriff im Zusammenhang mit Charakteren.

9.3. Satz und Def.: (a) Sei $\chi \neq \chi_0$ ein Charakter mod q. Dann gibt es eind. ein q^* mit: $q^* | q$ und q^* ist die kürzeste Periode von χ, eingeschränkt auf $\{n \in \mathbb{N};\ (n,q)=1\}$.

(b) Falls in (a) $q^* = q$ gilt, heißt χ primitiver Charakter.

(c) Zu jedem Charakter $\chi \neq \chi_0$ mod q gibt es eind. ein $q^* | q$ und einen primitiven Charakter χ^* mod q^*, so dass $\chi(n) = \chi^*(n)$ für $(n,q)=1$.
(D.h. $\chi = \chi^* \cdot \chi_0$.)

Man sagt, χ wird erzeugt vom primitiven Charakter χ^* mod q^*.
Die Zahl q^* heißt Führungszahl bzw. Erklärungsmodul zum Charakter χ mod q.

9.4. Bem.: χ_0 mod q wird nicht zu den primitiven Charakteren gezählt [obwohl χ_0 mod 1 alle χ_0 mod q erzeugt].

Bew.: Zu (a): Sei $q^* \leq q$ die kleinste nat. Zahl, für die χ auf $\{n;\ (n,q)=1\}$ q^*-periodisch ist (d.h. $\chi(n+r q^*) = \begin{cases} 0, & (n+r q^*, q) > 1, \\ \chi(n), & \text{sonst}; \text{"}=1 \end{cases}$).

Zeigen $q^* | q$: Seien $a, b \in \mathbb{Z}$ mit $(q, q^*) = a q + b q^*$ [Euklidischer Algorithmus].
Falls $(a + (q, q^*), q) = 1$, folgt $\chi(n + (q, q^*)) = \chi(n + aq + bq^*) = \chi(n + bq^*)$
$= \chi(n)$, so dass auch (q, q^*) Periode.

Also: $q^* \leq (q, q^*) \leq q^* \Rightarrow (q, q^*) = q^* \Rightarrow q^* | q$.

Zu (c): • Sei $q^* | q$ nach (a) die kleinste Periode von χ auf $\{n;\ (n,q)=1\}$.

• Es muss ein primitiver Charakter χ^* mod q^* gefunden werden, der χ erzeugt. Dazu muss $\chi^*(n) = \begin{cases} \chi(n), & (n,q)=1 \\ 0, & (n,q^*)>1 \end{cases}$ gesetzt werden. Es fehlen die Werte von $\chi^*(n)$ für $(n,q)>1$ und $(n,q^*)=1$.

Falls es $t \in \mathbb{Z}$ gibt mit $(n + tq^*, q) = 1$, setze $\chi^*(n) = \chi(n + tq^*)$.
Die Wahl von t darin ist unerheblich, da χ auf $\{n;\ (n,q)=1\}$ q^*-periodisch.

- Man kann $t = \prod_{\substack{p \mid q \\ p \nmid q^* m}} p$ nehmen, es genügt, z.z.: $m \nmid m + tq^*$ für alle $m \mid q$.
- 1. Fall: $m \mid q^*$. Aus $m \mid m + tq^*$ folgt $m \mid m$, im ↯ zu $(m, q^*) = 1$.
- 2. Fall: $m \nmid q^*$, $m \mid q$, $m \mid m$. Aus $m \mid m + tq^*$ folgt $m \mid tq^*$, $m \mid t$, im ↯ zur Def. von t.
- 3. Fall: $m \nmid q^*$, $m \mid q$, $m \nmid m$. Dann ist $m \mid t$, und aus $m \mid m + tq^*$ folgt $m \mid m$, ↯.
- Nun ist χ^* nach Def. q^*-periodisch. Weiter ist χ^* vollst. multiplikativ und somit Charakter mod q^*. Da q^* minimale Periode, ist (außer $q^* = 1$, $\chi^* = \mathbb{1}$) χ^* primitiver Charakter mod q^*. (Aus $\chi^* = \mathbb{1}$ folgt $\chi = \chi^*$ mod q, was ausgeschlossen war.) □

9.5 **Bsp.:** χ mod 10 wird erzeugt von χ^* mod 5:

$m\ (10)$	1	2	3	4	5	6	7	8	9
$\chi^*(m)$	1	i	$-i$	-1	0	1	i	$-i$	-1
$\chi(m)$	1	0	$-i$	0	0	0	i	0	-1

9.6 **Satz:** Sei $\chi \neq \chi_0$ mod q von χ^* erzeugt.

Dann gilt für $\sigma > 1$: $$L(s,\chi) = L(s,\chi^*) \cdot \prod_{p \mid q} \left(1 - \frac{\chi^*(p)}{p^s}\right).$$

Bew.: Für $\sigma > 1$ liefert der Euler-Π-Satz Anz 8.15

$$L(s,\chi) = \prod_{p \nmid q} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \nmid q} \left(1 - \frac{\chi^*(p)}{p^s}\right)^{-1} = \underbrace{\prod_p \left(1 - \frac{\chi^*(p)}{p^s}\right)^{-1}}_{= L(s,\chi^*)} \cdot \prod_{p \mid q} \left(1 - \frac{\chi^*(p)}{p^s}\right).$$ □

9.7 **Bem.:** Für den Hauptcharakter χ_0 mod q gilt für $\sigma > 1$:

$$L(s,\chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{\substack{p \\ p \nmid q}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{p \mid q} \left(1 - \frac{1}{p^s}\right) = \zeta(s) \prod_{p \mid q} \left(1 - \frac{1}{p^s}\right).$$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a10: Der Satz von Siegel

Stichworte: Satz von Siegel, Ineffektivität der Siegel-Konstanten, Beweis nach Estermann, nullstellenfreies Gebiet für $L(s,\chi)$

10.1. Einleitung: Im Beweis des Dirichletschen PZSes in a8 spielte die Aussage $L(1,\chi)\neq 0$ eine große Rolle. Diese muss für stärkere PZSätze verschärft werden, d.h. mit einer unteren Schranke >0 quantifiziert werden, was Siegel 1935 zeigte (und seither unverbessert ist):

10.2. Satz von Siegel: Sei $\chi\neq\chi_0$ ein reeller Charakter mod q und $\varepsilon>0$. Es existiert ein $\tilde{c}(\varepsilon)$, so dass $L(1,\chi)>\tilde{c}(\varepsilon)\cdot q^{-\varepsilon}$. [$\tilde{c}(\varepsilon)$ nur von ε abh.]

10.3. Bem.: Aus keinem bekannten Beweis kann eine effektive Abhängigkeit der Konstanten $\tilde{c}(\varepsilon)$ von ε (etwa in der Form $\tilde{c}(\varepsilon)\leq 100\varepsilon^{-5}$) entnommen werden. [Die einzig bekannte effektive Version lautet $L(1,\chi)\geq c\,q^{-1/2}$, c angebbar.] Jeder Satz, der im Beweis den Satz von Siegel verwendet, hat diesen Makel!

(nach T. Estermann)

10.4. Bew.: 1.) Es genügt, primitive χ mod q zu betrachten:
Sonst sei χ von χ^* mod q^* erzeugt, $1<q^*\mid q$. Sei die Beh. für χ^* schon gezeigt.

Wir haben $L(s,\chi)=L(s,\chi^*)\cdot\prod_{p\mid q}\left(1-\frac{\chi^*(p)}{p^s}\right)$ nach Satz 9.6.

Das $\prod$ ist $\geq\prod_{p\mid q}\left(1-\frac{1}{p}\right)\geq\prod_{p\leq q}\left(1-\frac{1}{p}\right)=\exp\left(\sum_{p\leq q}\log\left(1-\frac{1}{p}\right)\right)=\exp\left(-\sum_{p\leq q}\sum_{\ell\geq 1}\frac{1}{\ell p^\ell}\right)$

$\geq\exp(-\log\log(q)-D_1)=\frac{D_2}{\log(q)}$

mit $D_2>0$. Somit: $L(1,\chi)\geq L(1,\chi^*)\frac{D_2}{\log(q)}\geq\tilde{c}(\frac{\varepsilon}{2})q^{-\varepsilon/2}\frac{D_2}{\log(q)}\geq\tilde{c}(\varepsilon)q^{-\varepsilon}$.

2.) Seien χ_1 mod q_1 und χ_2 mod q_2 verschiedene, primitive reelle Charaktere. Dann: $\chi_1\chi_2 \neq \chi_0$ mod q_1q_2 ⌜Sonst $\chi_1=\chi_2$ mod q_1q_2. Dann folgt wie im Bew. von Satz 9.3 (a), dass q_1q_2, q_1, q_2 und (q_1,q_2) Perioden auf $\{n;\ (n,q_1q_2)=1\}$ sind. Die Primitivität zeigt $q_1=(q_1,q_2)=q_2$, $\chi_1=\chi_2$ ↯.⌟
Somit ist $F(s)=F(s,\chi_1,\chi_2):=\zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$ holomorph in $\{s,\ \sigma>0,\ s\neq 1\}$, F hat in $s=1$ Pol 1. Ordnung mit Residuum
$\lambda:=L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)\in\mathbb{R}$.

3.) Es gilt $F(\sigma)>\frac{1}{2}-\frac{c_1\lambda}{1-\sigma}(q_1q_2)^{4(1-\sigma)}$ für $\frac{7}{8}<\sigma<1$. "Estermanns Lemma"

3.1) Haben $F(s)=\sum_{n\geq 1}\frac{f(n)}{n^s}$ mit $f=\mathbb{1}*\chi_1*\chi_2*\chi_1\chi_2$ in $\sigma>1$.

Beh.: $\forall n: f(n)\geq 0$. Klar: $f(1)=1$, da f multiplikativ.

⌜Die Eulerprodukte der Faktoren von F zeigen für $\sigma>1$, dass
$$\log(F(s))=\sum_p\sum_{k\geq 1}\frac{1}{k}p^{-ks}\underbrace{\left(1+\chi_1(p^k)+\chi_2(p^k)+\chi_1\chi_2(p^k)\right)}_{=(1+\chi_1(p^k))\cdot(1+\chi_2(p^k))\geq 0},$$
also sind die Koeffizienten der Dirichletreihe von $\log(F(s))$ alle reell und ≥ 0, dasselbe gilt dann für die Koeffizienten von $F(s)=\exp(\log(F(s)))$, die $f(n)$.⌟

3.2) F kann um $s_0=2$ in eine Potenzreihe vom Kgz.radius 1 (Pol bei $s=1$) entwickelt werden: $F(s)=\sum_{\nu\geq 0}\alpha_\nu(2-s)^\nu$, $|2-s|<1$, mit $\forall\nu: \alpha_\nu\geq 0$, $\alpha_0=F(2)\geq f(1)=1$, denn $\alpha_\nu=(-1)^\nu\cdot\frac{F^{(\nu)}(2)}{\nu!}=\frac{(-1)^\nu}{\nu!}\sum_{k\geq 1}(-1)^\nu\frac{f(k)\log^\nu(k)}{k^2}\geq 0$ für $f(k)\geq 0$. Nun gilt:
$F(s)-\frac{\lambda}{s-1}$ ist holomorph in $\{s;\ |s-2|<2\}$, haben somit
$$F(s)-\frac{\lambda}{s-1}=\sum_{\nu\geq 0}(\alpha_\nu-\lambda)(2-s)^\nu \text{ für } |s-2|<2. \quad (*)$$

3.3) Mit $|\sum_{A<n<B}\chi(n)|\leq\varphi(q)$ für χ mod q zeigt part. $\sum$: $L(s,\chi)=s\int_1^\infty\left(\sum_{n\leq u}\chi(n)\right)u^{-s-1}du$
$$\Rightarrow L(s,\chi)\ll\int_1^q u^{-\sigma}du+q\int_q^\infty u^{-\sigma-1}du\ll\frac{q^{1-\sigma}}{1-\sigma}+q\cdot\frac{q^{-\sigma}}{\sigma}\ll q^{1/2} \text{ für } \sigma\geq\tfrac{1}{2} \text{ und } \sigma\leq\tfrac{7}{2}.$$
Also: $L(s,\chi_j)\ll q_j^{1/2}$ für $j=1,2$, $L(s,\chi_1\chi_2)\ll q_1^{1/2}q_2^{1/2}$ für $|s-2|\leq\frac{3}{2}$,
also $|\lambda|\ll q_1q_2$. Mit $\zeta(s)\ll 1$ für $|s-2|=\frac{3}{2}$ zeigt dies
$$F(s)-\frac{\lambda}{s-1}\ll q_1q_2 \text{ für } |s-2|=\tfrac{3}{2}.$$
Die Koeff. $\alpha_\nu-\lambda$ der Potenzreihe in $(*)$ erfüllen mit der Cauchyformel daher die Ungl. $|\alpha_\nu-\lambda|\ll q_1q_2\cdot\left(\frac{2}{3}\right)^\nu$.

↳ ⌜$\frac{1}{n!}|f^{(n)}(z_0)|\leq\frac{1}{r^n}\max_{|z-z_0|=r}|f(z)|$⌟

3.4) Sei nun $\frac{7}{8} \le \sigma < 1$. Mit (später zu wählendem) $N = N(q_1, q_2)$ folgt

$$\sum_{\nu \ge N} |\alpha_\nu - \lambda| (2-\sigma)^\nu \ll q_1 q_2 \sum_{\nu \ge N} \left(\tfrac{2}{3}\right)^\nu \left(\tfrac{9}{8}\right)^\nu \ll q_1 q_2 \left(\tfrac{3}{4}\right)^N \ll q_1 q_2 e^{-N/4}.$$

Dies liefert

$$F(\sigma) - \frac{\lambda}{\sigma - 1} \ge \sum_{0 \le \nu \le N-1} (\alpha_\nu - \lambda)(2-\sigma)^\nu - C q_1 q_2 e^{-N/4}$$

$$\ge 1 - \lambda \frac{(2-\sigma)^N - 1}{1-\sigma} - C q_1 q_2 e^{-N/4}. \quad \text{[alle } \alpha_\nu \ge 0,\ \alpha_0 = 1\text{]}$$

sei C hier die impl. Konstante, $C > 1$.

Bestimme jetzt N so, dass $\frac{1}{2} e^{-N/4} < C \cdot q_1 q_2 e^{-N/4} < \frac{1}{2}$ ist,

insb. $N \le 4 \log(q_1 q_2) + C_0$ und $(2-\sigma)^N = \exp(N \log(1 + (1-\sigma))) < \exp(N(1-\sigma)) \ll (q_1 q_2)^{4(1-\sigma)}$.

Man erhält

$$F(\sigma) > 1 - C_1 \frac{\lambda}{1-\sigma} (q_1 q_2)^{4(1-\sigma)} - \frac{1}{2} = \frac{1}{2} - C_1 \frac{\lambda}{1-\sigma} (q_1 q_2)^{4(1-\sigma)},$$ die Beh. 3).

4.) Zeige nun Siegels Unglg. für $\chi_2 \bmod q_2$. Dazu sei $\varepsilon > 0$. Nimm folgendes $\chi_1 \bmod q_1$:

4.1) 1. Fall: $\exists\, q_1^*$, primitives $\chi_1^* \bmod q_1^*$ mit $\chi_1^* \ne \chi_0$, $\chi_1^2 = \chi_0$ und $L(\sigma_1, \chi_1) = 0$ für ein $\sigma_1 = \sigma_1(\varepsilon) \in (1 - \frac{\varepsilon}{16}, 1)$.

Definiere F mit diesem χ_1. Für jedes zulässige χ_2 gilt $F(\sigma_1) = F(\sigma_1, \chi_1, \chi_2) = 0$.

4.2) 2. Fall: es ex. kein q_1, χ_1 wie im 1. Fall. Fixiere irgendein q_1, ein $\chi_1 \bmod q_1$ mit $\chi_1 \ne \chi_0$, $\chi_1^2 = \chi_0$. Wegen $L(\sigma, \chi_1)$, $L(\sigma, \chi_2)$, $L(\sigma, \chi_1\chi_2) \xrightarrow[\sigma \to \infty]{} 1$, wegen der Reellwertigkeit und Nichtverschwinden bei $\sigma > 1 - \frac{\varepsilon}{8}$ ist

$$L(\sigma, \chi_1) L(\sigma, \chi_2) L(\sigma, \chi_1\chi_2) > 0 \quad \text{für } \sigma \in (1 - \tfrac{\varepsilon}{8}, 1).$$

Da $\zeta(\sigma)$ beim Durchqueren des Pols das VZ wechselt ($\zeta(\sigma) < 0$ für $0 < \sigma < 1$), findet sich ein $\sigma_1 = \sigma_1(\varepsilon) \in (1 - \frac{\varepsilon}{8}, 1)$ mit $F(\sigma_1) < 0$ für alle zulässigen χ_2.

4.3) Aus 3.) ergibt sich bei festem $\sigma_1(\varepsilon)$, $\chi_1 \bmod q_1$ und bel. $\chi_2 \bmod q_2 > q_1$, dass

$$\frac{C_1 \lambda}{1-\sigma_1} (q_1 q_2)^{4(1-\sigma_1)} > \frac{1}{2} - F(\sigma_1) \ge \frac{1}{2}$$

bzw. $\lambda \gg (1-\sigma_1)(q_1 q_2)^{4(1-\sigma_1)}$.

Da $L(1, \chi_1) L(1, \chi_1\chi_2) \ll \log(q_1) \cdot \log(q_1 q_2) \ll_\varepsilon \log(q_2)$ ($q_1 = q_1(\varepsilon)$) (vgl. Ü A1 Bl. 7; wie in 3.3),

folgt $L(1, \chi_2) \gg_\varepsilon q_2^{4(1-\sigma_1)} \log^{-1}(q_2) \gg_\varepsilon q_2^{-\varepsilon/2} \log^{-1}(q_2) \gg_\varepsilon q_2^{-\varepsilon}$.

Dies gilt für alle zulässigen χ_2 mit $q_2 > q_1(\varepsilon)$, durch ev. Verkleinern der impliziten Konstanten kann die Unglg. für alle q_2 gezeigt werden. □

Wir wollen nun eine möglichst starke Version des PZSes in APs zeigen, wobei die Gleichmäßigkeit in einem möglichst großen q-Bereich kontrolliert werden soll. Dazu muss auch ein möglichst großes nullstellenfreies Gebiet für $L(s, \chi)$ hergeleitet werden.

So wie wir für den Beweis des PZSes zuerst die Abschätzung 4.6 für ζ benötigt haben, muss eine solche auch für L-Funktionen gezeigt werden, was wir ähnlich wie dort zeigen. Dabei muss der Fall $\chi=\chi_0$ von $\chi\neq\chi_0$ unterschieden werden.

10.4. **Def.:** Sei $q\in\mathbb{N}$, χ Charakter mod q, dann sei $E(q,\chi):=\begin{cases}1, & \chi=\chi_0,\\ 0, & \text{sonst.}\end{cases}$

10.5. **Satz:** Sei $q\in\mathbb{N}$, χ Charakter mod q, $M\in\mathbb{N}$. Dann gilt für $s=\sigma+it$ mit $\sigma>-M$, dass $L(s,\chi)-E(q,\chi)\cdot\frac{\varphi(q)}{q(s-1)}=\mathcal{O}_M(|s|^{M+1}q^{M+2})$.

Bew.: Laut Eulerscher Summenformel Satz 1.6 erhalten wir für $a\in\mathbb{Z}$:

$$\sum_{m=0}^{\infty}(qm+a)^{-s}=\int_0^\infty(qu+a)^{-s}du-qs\int_0^\infty(qu+a)^{-s-1}P_0(u)du-\tfrac12 a^{-s},\quad P_0(u)=u-\lfloor u\rfloor-\tfrac12,$$

$$=\frac{a^{-s+1}}{s-1}-\frac{a^{-s}}{2}-qs\int_0^\infty(qu+a)^{-s-1}P_0(u)du.$$

Def. Fkt. P_ℓ für $\ell\in\mathbb{N}$ durch $P_{\ell+1}'(u)=P_\ell(u)$ und $\int_0^1P_\ell(u)du=0$, dann gilt partielle $\int$:

$$\int_0^\infty(qu+a)^{-s-1}P_0(u)du=\tfrac12 q(s+1)(qu+a)^{-s-2}\Big|_0^\infty-\sum_{\ell\geq2}\ell!\,P_\ell(0)q^\ell a^{-s-\ell-1}$$
$$+q^M(s+1)\cdots(s+M)\int_0^\infty(qu+a)^{-s-M-1}du,$$

also $$\sum_{m=0}^{\infty}(qm+a)^{-s}=\frac{a^{-s+1}}{s-1}-\frac{a^{-s}}{2}-\sum_{\ell=2}^{M-1}\ell!\,P_\ell(0)q^\ell a^{-s-\ell}+q^{M+1}s(s+1)\cdots(s+M)\underbrace{\int_0^\infty(qu+a)^{-s-M-1}P_M(u)du}_{=:f(s),\ \text{in } \mathrm{Re}(s)>-M \text{ holomorph}},$$

Somit: $\sum_{m=0}^{\infty}(qm+a)^{-s}-\frac{a^{-s+1}}{s-1}=\mathcal{O}_M(q^{M+1}|s|^{M+1})$.

Wegen der ONR $\sum_{a=1}^{q}\chi(a)=E(q,\chi)\varphi(q)$ erhalten wir $\sum_{a=1}^{q}\chi(a)\frac{a^{-s+1}}{s-1}=E(q,\chi)\frac{\varphi(q)}{s-1}+\underbrace{h(q,\chi,s)}_{=\mathcal{O}(q^{M+2}),\ \text{holomorph}}$

für $\mathrm{Re}(s)>-M$ also $L(s,\chi)-E(q,\chi)\frac{\varphi(q)}{q(s-1)}=\mathcal{O}_M(|s|^{M+1}q^{M+2})$. □

10.6. **Def.:** Für $q\in\mathbb{N}$ und $t\in\mathbb{R}$ sei $\mathcal{L}:=\log(q)+\log(|t|+2)$.

Es sei χ ein Charakter mod q und $T>0$. Dann bezeichne

$$N(T,\chi):=\#\{\rho=\beta+i\gamma;\ L(\rho,\chi)=0,\ 0\leq\gamma<T,\ 0\leq\beta\leq1\}$$

die Anzahl der Nullstellen von $L(s,\chi)$ im kritischen Streifen mit Imaginärteil $<T$ (und ≥0).

Wir benötigen die folgende Version von Lemma 4.4 für L-Funktionen.

10.7. **Lemma:** Sei $q\in\mathbb{N}$, χ Charakter mod q, $T\geq0$, $m\in\mathbb{N}$. Dann ist

(i) $N(T+1,\chi)-N(T,\chi)=\mathcal{O}(\mathcal{L})$,

(ii) Für alle $s=\sigma+it$ mit $\sigma\geq-m$ gilt

$$-\frac{L'}{L}(s,\chi)=\frac{E(q,\chi)}{s-1}-\sum_{\substack{\rho,\ L(\rho,\chi)=0\\ |\mathrm{Im}(\rho)-t|\leq1}}\frac{1}{s-\rho}+\mathcal{O}_m(\mathcal{L}).$$

Bew.: Wenden Lemma 4.4 an auf

$$f(s) := (s-1)^{E(q,\chi)} L(s,\chi), \quad s_0 := 2+iT, \quad r = 4(m+3).$$

Haben $|f(s_0)| = |(s_0-1)|^{E(q,\chi)} \prod_p \frac{1}{|1-\chi(p)p^{-s_0}|} \geq \prod_p \frac{1}{1+p^{-2}} \gg 1.$

$\hookrightarrow L(s,\chi) \ll |s|^{m+1} q^{m+2} \leq (qT)^{2m+3}$

Nach Satz 10.5 sind die Vor. von Lemma 4.4 mit $M = 4(m+3)\mathcal{L}$ erfüllt.

Dies ergibt für $|s-s_0| \leq m+3$ dann

$$(\sigma > -m-1) \qquad \circledast \quad \frac{L'}{L}(s,\chi) + \frac{E(q,\chi)}{s-1} - \sum_\rho \frac{1}{s-\rho} = O_m(\mathcal{L}),$$

wobei ρ alle Nullstellen von $L(s,\chi)$ mit $|\rho - s_0| \leq 2(m+3)$ entsprechend Vielfachheit durchläuft.

- Wende $\circledast$ zunächst mit $s = s_0$ und $m = 2$ an.

  Wegen $\frac{L'}{L}(s_0,\chi) = O(1)$ und $\frac{E(q,\chi)}{s_0-1} = O(1)$ erhalten wir damit

  $$\oplus \quad \mathrm{Re}\Big(\sum_{|\rho-s_0|\leq 10} \frac{1}{s_0-\rho}\Big) = O(\mathcal{L}).$$

  Für $\rho = \beta + i\gamma$ ist

  $$\mathrm{Re}\Big(\frac{1}{s_0-\rho}\Big) = \mathrm{Re}\Big(\frac{\overline{s_0-\rho}}{|s_0-\rho|^2}\Big) = \frac{2-\beta}{|s_0-\rho|^2}.$$ Es ist $2-\beta \geq 1$ und $|s_0-\rho|^2 \leq 100$,

  also $\mathrm{Re}\Big(\frac{1}{s_0-\rho}\Big) \geq \frac{1}{100}$, es folgt mit $\oplus$, dass $N(T+1,\chi) - N(T,\chi) = O(\mathcal{L})$, also (i).

- Mit $\circledast$ folgt schließlich für $|s-s_0| \leq m+2$, dass $\leftarrow \sigma \geq 2-(m+2) = -m$

  $$\Big|\frac{L'}{L}(s,\chi) + \frac{E(q,\chi)}{s-1} - \sum_{|\rho-s_0|\leq 1} \frac{1}{s-\rho}\Big| = O_m(\mathcal{L}) + O_m\Big(\sum_{1\leq|\rho-s_0|\leq 2(m+3)} \frac{1}{s-\rho}\Big) = O_m(\mathcal{L}),$$

  also (ii). □

Mit Lemma 10.7 gelingt nun ein wesentlicher Satz über nullstellenfreie Gebiete von $L(s,\chi)$. Dieser lässt noch den Fall $\chi^2 = \chi_0$, $|\tau|$ klein, offen, was wir erst in a11 behandeln (unter Verwendung des Satzes von Siegel 10.2).

10.8. Satz (nullstellenfreies Gebiet für L-Funktionen):

(i) Es sei $\chi^2 \neq \chi_0$ (d.h. χ komplex) oder $|t| \geq 1$. Dann gibt es eine absolute Konstante $c_0 > 0$ so, dass $L(s,\chi) \neq 0$ für $\sigma \geq 1 - 2c_0\mathcal{L}^{-1}$ gilt. Für $\sigma \geq 1 - c_0\mathcal{L}^{-1}$ ist $\frac{L'}{L}(s,\chi) = O(\mathcal{L}^2)$.

(ii) Es sei $\chi^2 = \chi_0$ (d.h. χ reell). Dann gibt es eine absolute Konstante $c_1 > 0$ mit folgender Eigenschaft: Es sei $0 < \delta < c_1$ und $\rho = \beta + i\gamma$ beliebige Nullstelle von $L(s,\chi)$ mit $|\gamma| \geq \frac{\delta}{\log(q)}$, dann ist $\beta \leq 1 - \frac{\delta}{R\mathcal{L}}$ für eine absolute Konstante $R > 0$.

Für $\sigma \geq 1 - \frac{\delta}{10\mathcal{L}}$ gilt dann $\frac{L'}{L}(s,\chi) = O(\mathcal{L}^2)$.

Bew.: Zu (i): Angenommen, $\rho_0 = \beta_0 + i\gamma_0$ sei Nst. der Ordnung $m \geq 1$ von $L(s,\chi)$,
wo $\gamma_0 \geq 0$, $\beta_0 = 1 - \frac{d_0}{\mathcal{L}_\gamma}$ mit $d_0 > 0$, $\mathcal{L}_\gamma = \log(q) + \log(\gamma_0 + 2)$.

Setzen

$$h(\sigma,\chi) = 3\frac{L'}{L}(\sigma,\chi_0) + 4\frac{L'}{L}(\sigma+i\gamma_0,\chi) + \frac{L'}{L}(\sigma+2i\gamma_0,\chi^2) \text{ und } \sigma_0 := 1 + \frac{4d_0}{\mathcal{L}_\gamma}.$$

Für $\sigma > 1$ ist $\frac{L'}{L}(\sigma,\chi_0) = \frac{\zeta'}{\zeta}(\sigma) + O\Big(\sum_{p|q} \log(p) p^{-\sigma} \sum_{m\geq 0} p^{-m\sigma}\Big) = \frac{\zeta'}{\zeta}(\sigma) + O(\log(q))$ laut Satz 8.6.
und damit $\frac{L'}{L}(\sigma_0,\chi_0) = -\frac{1}{\sigma_0 - 1} + O(\mathcal{L}_\gamma)$. ⊕

Wende nun Lemma 4.5 an mit $s_0 = \sigma_0 + i\gamma_0$, $r = \frac{1}{2}$, $f(s) = L(s,\chi)$,
und mit $s_0' = \sigma_0 + 2i\gamma_0$, $r = \frac{1}{2}$, $f(s) = L(s,\chi^2)$ an.

Für absolute Konstanten $c_1, c_2, \ldots > 0$ gilt
wegen $|L(\sigma_0 + i\gamma_0,\chi)| \geq \prod_p \frac{1}{1+p^{-\sigma_0}} \geq \zeta(\sigma_0)^{-1} \geq \frac{c_1}{\sigma_0 - 1} = \frac{c_1 \mathcal{L}_\gamma}{4d_0}$
bzw. $|L(\sigma_0 + 2i\gamma_0,\chi^2)| \geq \prod_p \frac{1}{1+p^{-\sigma_0}} \geq \frac{c_1}{\sigma_0 - 1} = \frac{c_1 \mathcal{L}_\gamma}{4d_0}$
dann $\left|\frac{f(s)}{f(s_0)}\right| \leq e^K$ bzw. $\left|\frac{f(s)}{f(s_0')}\right| \leq e^K$ mit $K \leq c_2 \mathcal{L}$. ⌜Denn $L(s,\chi) \ll e^{B\mathcal{L}_\gamma}$ für ein $B > 0$, alle s nahe s_0, s_0'.
(Mit Satz 10.5, wie im Bew. von 10.7)⌟

Dann ergibt Lemma 4.5, dass

$$-\mathrm{Re}\left(\frac{L'}{L}(\sigma_0 + i\gamma_0,\chi)\right) < c_2 \mathcal{L}_\gamma - \frac{1}{\sigma_0 - \beta_0} \quad \text{⌜wegen Nst. } \rho_0 \text{ laut Ann.⌟}$$

sowie $-\mathrm{Re}\left(\frac{L'}{L}(\sigma_0 + 2i\gamma_0,\chi^2)\right) < c_3 \mathcal{L}_\gamma$.

Dies ergibt mit ⊕, dass $\mathrm{Re}(h(\sigma_0,\chi)) \geq -\frac{3}{\sigma_0 - 1} + \frac{4}{\sigma_0 - \beta_0} - c_4 \mathcal{L}_\gamma$

$$= -3 \cdot \frac{\mathcal{L}_\gamma}{4d_0} + 4 \cdot \frac{\mathcal{L}_\gamma}{5d_0} - c_4 \mathcal{L}_\gamma = \Big(\frac{1}{20d_0} - c_4\Big)\mathcal{L}_\gamma$$

> 0 für $d_0 > 0$ klein.

Aus der Darstellung $\mathrm{Re}(h(\sigma_0,\chi)) = -\sum_{n\geq 1} \Lambda(n) n^{-\sigma_0} \chi_0(n) \cdot (3 + 4\cos(\theta_n) + \cos(2\theta_n))$ mit
$\chi(n) e^{-i\gamma_0 \log(n)} = \cos(\theta_n) + i\sin(\theta_n)$ erhalten wir $\mathrm{Re}(h(\sigma_0,\chi)) \leq 0$, was für hinreichend kleine d_0
im ↯ zu vorigem steht. Dies zeigt die behauptete Nullstellenfreiheit.

- Es sei nun $s = \sigma + it$ mit $\sigma \geq 1 - \frac{c_0}{\mathcal{L}}$. Nach Lemma 10.7 (ii) haben wir

$$-\frac{L'}{L}(s,\chi) = \frac{E(q,\chi)}{s-1} - \sum_{\substack{\rho,\, L(\rho,\chi)=0 \\ |\mathrm{Im}(\rho)-t| \leq 1}} \frac{1}{s-\rho} + O_m(\mathcal{L}),$$

und laut eben gezeigter Nullstellenfreiheit
haben wir $\frac{1}{|s-\rho|} = O(\mathcal{L})$. ⌜Denn $L(s,\chi) \neq 0$ für $\sigma \geq 1 - \frac{2c_0}{\mathcal{L}}$ zeigt $\mathrm{Re}(\rho) < 1 - \frac{2c_0}{\mathcal{L}}$,
aber $\sigma > 1 - \frac{c_0}{\mathcal{L}} \Rightarrow |s-\rho| \gg \mathcal{L}^{-1}$.⌟ Die Anzahl der Summanden ist laut 10.7 (i)
nun $\ll N(t+1,\chi) - N(t,\chi) = O(\mathcal{L})$, es folgt der Zusatz über $\frac{L'}{L}$.

Zu (ii): OE sei $\chi \neq \chi_0$, da $L(s,\chi_0)$ in $s=1$ einen Pol 1. Ordnung hat.
Angenommen, $s_1 = \beta_1 + i\gamma_1$ sei Nullstelle der Ordnung $m_1 \geq 1$ von $L(s,\chi)$, wobei $\gamma_1 = \frac{d_1\delta}{\log(q)}$ mit $d_1 \geq 1$ und $\beta_1 = 1 - \frac{d_2\delta}{\log(q)}$ gelte. Setze $\sigma_1 := 1 + \frac{4d_2\delta}{\log(q)}$,

und $\mathcal{L}_{\gamma_1} = \log(q) + \log(\gamma_1 + 2) \ll \log(q) = \mathcal{L}$.

Wende nun Lemma 4.5 an mit $s_1 = \sigma_1 + i\gamma_1$, $r = \frac{1}{2}$, $f(s) = L(s,\chi)$,
und mit $s_1' = \sigma_1 + 2i\gamma_1$, $r = \frac{1}{2}$, $f(s) = L(s,\chi^2)\cdot(s-1)$ an. ($\chi^2 = \chi_0$)

Dies ergibt $-\mathrm{Re}\left(\frac{L'}{L}(\sigma_1 + i\gamma_1, \chi)\right) < c_5\mathcal{L} - \frac{1}{\sigma_1 - \beta_1}$ [wegen Nst. s_1 nahe s_1 laut Ann.]

bzw. $-\mathrm{Re}\left(\frac{L'}{L}(\sigma_1 + 2i\gamma_1, \underbrace{\chi^2}_{=\chi_0}) + \frac{1}{\sigma_1 - 1 + 2i\gamma_1}\right) < c_6\mathcal{L}$, [bei 2. Version]

d.h. $-\mathrm{Re}\left(\frac{L'}{L}(\sigma_1 + 2i\gamma_1, \chi^2)\right) < c_6\mathcal{L} + \mathrm{Re}\frac{1}{\sigma_1 - 1 + 2i\gamma_1}$.

Ann.: $d_1 \geq 5d_2$

Mit $\gamma_1 = \frac{d_1\delta}{\mathcal{L}}$ folgt $\mathrm{Re}\frac{1}{\sigma_1 - 1 + 2i\gamma_1} = \frac{\sigma_1 - 1}{(\sigma_1-1)^2 + 4\gamma_1^2} = \frac{\sigma_1 - 1}{(\sigma_1-1)^2 + 4\delta^2/\mathcal{L}^2} = \frac{d_2}{4d_2^2 + d_1^2}\cdot\frac{\mathcal{L}}{\delta} \leq \frac{\mathcal{L}}{29 d_2\delta}$

wir erhalten $\mathrm{Re}(h(\sigma_1,\chi)) \geq -\frac{3}{\sigma_1 - 1} + \frac{4}{\sigma_1 - \beta_1} - \mathrm{Re}\frac{1}{\sigma_1 - 1 + 2i\gamma_1} - c_7\mathcal{L} = -\frac{3\mathcal{L}}{4d_2\delta} + \frac{4\mathcal{L}}{5d_2\delta} - \frac{\mathcal{L}}{29d_2\delta} - c_7\mathcal{L}$

$= \underbrace{\left(-\frac{3}{4} + \frac{4}{5} - \frac{1}{29}\right)}_{>0}\frac{\mathcal{L}}{d_2\delta} - c_7\mathcal{L}$

was wieder im ↯ zu $\mathrm{Re}(h(\sigma_1,\chi)) \leq 0$ für hinreichend kleine d_2 steht.

Also folgt $d_2 > \frac{1}{5}d_1 \geq \frac{1}{5}$ und $\beta_1 = 1 - \frac{d_2\delta}{\log(q)} < 1 - \frac{d_1\delta}{5\log(q)}$, nimm $R = \frac{5}{d_1}$.

- Der Zusatz über $\frac{L'}{L}$ folgt genau wie in (i).

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a11: Siegelnullstellen

Stichworte: Siegelnullstellen, Satz von Siegel-Walfisz, β-Term in expliziten Formeln

---

11.1. Einleitung: Aus $L(1,\chi)\neq 0$ bzw. dem Satz von Siegel folgt lediglich die Existenz einer Umgebung U von $s=1$ mit $L(s,\chi)\neq 0$ für $s\in U$. Über die Größe von U ist so nichts bekannt, insb. nicht über ihre Größe in Abh. von q. Dieser Mangel wird zunächst behoben. Danach untersuchen wir Siegel-Nullstellen bzw. Ausnahme-/exzeptionelle Nullstellen, deren potentielle Existenz bis heute nicht ausgeschlossen werden kann. Immerhin können wir zeigen, dass ihr Auftreten sehr selten ist. Damit können wir den besten PZS in APs zeigen, der eine Kontrolle über die q-Abhängigkeit des Fehlerterms zulässt: den Satz von (Page-) Siegel-Walfisz 11.6.

11.2. Satz: Sei $q\in\mathbb{N}$, χ ein Charakter mod q. Dann gibt es eine absolute Konstante $c_0>0$, so dass im Gebiet $|t|<1$ und $\sigma>1-\frac{c_0}{\log(q)}$ höchstens eine Nullstelle von $L(s,\chi)$ liegt, die im Falle ihrer Existenz notwendig reell und einfach ist.

11.3. Bew.: Wir zeigen dafür, dass $c_0>0$ ex. so, dass für $q\geq q_0$ die Fkt. $L(s,\chi)$ im Gebiet $\mathcal{G}=\{s=\sigma+it;\ \sigma>1-\frac{c_0}{\log(q)},\ |t|<\frac{c_0}{2\log(q)}\}$ höchstens eine Nullstelle besitzt. [Rest folgt mit Satz 10.8(ii)]

Wegen $\frac{L'}{L}(s,\chi_0)=\frac{\zeta'}{\zeta}(s)+O(\log(q))=-\frac{1}{s-1}+O(\log(q))$

können wir $\chi\neq\chi_0$ annehmen.

Nach Satz 10.8 können wir ferner auch $\chi^2=\chi_0$ annehmen.

Nach Lemma 10.7 haben wir

$$-\frac{L'}{L}(s,\chi)=-\sum_{\substack{\rho,\ L(\rho,\chi)=0\\ |\mathrm{Im}(\rho)-t|\leq 1}}\frac{1}{s-\rho}+R(s,\chi), \qquad \otimes$$

wo $|R(s,\chi)|\leq C\mathcal{L}$ gilt für eine absolute Konstante $C>0$.

- Wir nehmen an, $L(s,\chi)$ habe die Nst. $\rho_1=\beta_1+i\gamma_1$ mit $\beta_1>1-\frac{c_0}{\log(q)}$, $|\gamma_1|<\frac{c_0}{2\log(q)}$.

Falls $\rho_1 \notin \mathbb{R}$ ist auch $\bar{\rho}_1$ Nst., und haben dann für $\sigma_0 = 1 + \frac{2c_0}{\log(q)}$,

dass $\frac{1}{\sigma_0-\beta_1-i\gamma_1} + \frac{1}{\sigma_0-\beta_1+i\gamma_1} = \frac{2(\sigma_0-\beta_1)}{(\sigma_0-\beta_1)^2+\gamma_1^2} = \frac{2}{\sigma_0-\beta_1}\cdot\frac{1}{1+\frac{\gamma_1^2}{(\sigma_0-\beta_1)^2}} > 0.$

Mit $0 < \gamma_1 \le \frac{1}{2}(\sigma_0-1) \le \frac{1}{2}(\sigma_0-\beta_1)$ folgt $\frac{2}{\sigma_0-\beta_1}\cdot\frac{1}{1+\frac{\gamma_1^2}{(\sigma_0-\beta_1)^2}} \ge \frac{2}{\sigma_0-\beta_1}\cdot\frac{1}{1+1/4} \ge \frac{8}{5}\cdot\frac{\log(q)}{3c_0}$.

Wende nun $\otimes$ an mit $s=\sigma_0$, dies ergibt

$$-\mathrm{Re}\,\frac{L'}{L}(\sigma_0,\chi) \le -\frac{8}{15}\cdot\frac{\log(q)}{c_0} + \mathrm{Re}(R(\sigma_0,\chi)),$$ falls mindestens eine der Nst. $\notin \mathbb{R}$ ist.

Andererseits ist $-\mathrm{Re}\,\frac{L'}{L}(\sigma_0,\chi) = \sum_{n\ge 1}\Lambda(n)\chi(n)n^{-\sigma_0} \ge \frac{\zeta'}{\zeta}(\sigma_0) \ge -\frac{\log(q)}{2c_0} + O(1)$,

was im $\lightning$ zu vorigem steht, wenn $q \ge q_0$, denn $-\frac{1}{2} > -\frac{8}{15}$.

- Wir nehmen ferner an, $L(s,\chi)$ habe zwei reelle Nst. ρ_1, ρ_2 in $\mathcal{G}$ (nicht notwendig verschieden).

Dann ist $\frac{1}{\sigma_0-\beta_1} + \frac{1}{\sigma_0-\beta_2} = \frac{2\sigma_0-\beta_1-\beta_2}{(\sigma_0-\beta_1)(\sigma_0-\beta_2)}$, und wären $\beta_1, \beta_2 > 1 - \frac{c_0/2}{\log(q)}$, folgte

$$\frac{2\sigma_0-\beta_1-\beta_2}{(\sigma_0-\beta_1)(\sigma_0-\beta_2)} \ge (2\sigma_0-\beta_1-\beta_2)\cdot\frac{\log(q)}{3c_0}\cdot\frac{1}{\sigma_0-\beta_1} \ge \frac{4c_0}{\log(q)}\cdot\frac{\log(q)}{5c_0/2}\cdot\frac{1}{\sigma_0-\beta_1} = \frac{8}{5}\cdot\frac{1}{\sigma_0-\beta_1} \ge \frac{8}{5}\cdot\frac{\log(q)}{5c_0/2} = \frac{16}{25}\cdot\frac{\log(q)}{c_0}$$

$$\Rightarrow -\frac{\log(q)}{2c_0} + O(1) \le -\mathrm{Re}\,\frac{L'}{L}(\sigma_0,\chi) \le -\frac{16}{25}\cdot\frac{\log(q)}{c_0},$$ $\lightning$ wenn $q \ge q_0$, denn $-\frac{1}{2} > -\frac{16}{25}$.

$\rightsquigarrow c_0$ anpassen. $\square$

11.4 **Def.:** Sei $q \in \mathbb{N}$, χ ein Charakter mod q und $c_0 > 0$ fest. Die einzige möglicherweise existierende einfache reelle Ausnahmenullstelle β von $L(s,\chi)$, für die die Abschätzung $\beta \ge 1 - \frac{c_0}{\log(q)}$ gilt, heißt auch Siegel-Nullstelle / Siegel-Landau-Nst, bzw. exzeptionelle Nullstelle von $L(s,\chi)$. Der zugeh. Char. χ heißt Ausnahmecharakter.

11.5 **Bem.:** Es wird vermutet, dass Siegel-Nullstellen nicht existieren. Wesentlich stärker ist die verallgemeinerte Riemannsche Vermutung (GRH), nach der $\left(L(s,\chi)=0 \text{ mit } 0<\mathrm{Re}(\sigma)<1 \Rightarrow \mathrm{Re}(\sigma)=\frac{1}{2}\right)$ gilt für (jede Fkt.) $L(s,\chi)$.

Da Siegel-Nullstellen bis heute nicht ausgeschlossen werden können, muss buchstäblich mit ihnen gerechnet werden, vor allem in den expliziten Formeln in 11.11.

Wir tragen nun alle Erkenntnisse zusammen, um den folgenden PZS in APs zu zeigen:

11.6 **Satz** (Primzahlsatz von (Page-) Siegel-Walfisz): Es sei $A > 0$ beliebig groß, $q \in \mathbb{N}$, $(a,q)=1$ und $1 \le q \le \log^A(x)$. Dann ex. eine absolute Konstante $c > 0$ mit

(i) $\psi(x,\chi) = O_A\left(x\cdot\exp(-c\sqrt{\log(x)})\right)$ für jeden Charakter $\chi \ne \chi_0$ mod q,

(ii) $\psi(x;q,a) = \frac{x}{\varphi(q)} + O_A\left(x\cdot\exp(-c\sqrt{\log(x)})\right)$,

(iii) $\pi(x;q,a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O_A\left(x\cdot\exp(-c\sqrt{\log(x)})\right)$.

also $A \geq \frac{\log(q)}{\log\log(x)}$.

Bew.: Zu (i): Sei χ ein Charakter mod $q \leq \log^A(x)$, und OE sei $x = m + \frac{1}{2}$ mit $m \in \mathbb{N}$.

Wir setzen $c = 1 + \frac{1}{\log(x)}$ und $T = \exp(\sqrt{\log(x)})$.

Nach der Perronschen Formel Satz 3.12

gilt $\psi(x,\chi) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(-\frac{L'}{L}(s,\chi)\right) \frac{x^s}{s}\, ds + O\left(x \exp(-\sqrt{\log(x)}) \cdot \log^2(x)\right)$.

Nach Satz 10.8 (i) gibt es eine absolute Konstante $c_0 > 0$ mit $L(s,\chi) \neq 0$

und $\frac{L'}{L}(s,\chi) = O(\log^2(x))$ für $\sigma \geq 1 - \frac{c_0}{\log(x)}$ und $1 \leq |t| \leq T$.

Nach Satz 11.2 gibt es eine absolute Konstante $c_1 > 0$, so dass im Gebiet

$\sigma > 1 - \frac{c_1}{\log(q)}$ und $|t| < 1$ die Fkt. $L(s,\chi)$ höchstens eine reelle Nst. β besitzt.

Sei $\varepsilon = \frac{1}{2A}$. Nach dem Satz 10.2 von Siegel gilt $L(1,\chi) > \tilde{c}(\varepsilon) q^{-\varepsilon}$ für eine Konstante $\tilde{c}(\varepsilon) > 0$.

(*) Der MWS zeigt dann, dass $L(\sigma,\chi) \neq 0$ für $\sigma > 1 - q^{-\varepsilon}$ und alle $q > q_0(\varepsilon)$ gilt:

$L(\sigma,\chi) = L(1,\chi) - (1-\sigma) L'(\tilde{\sigma},\chi)$ mit $\sigma \leq \tilde{\sigma} \leq 1$. Man kann zeigen (vgl. Ü A2 Bl. 7),

dass für $1 - q^{-\varepsilon} \leq \tilde{\sigma} \leq 1$ nun $L'(\tilde{\sigma},\chi) = O(\log^2(2q))$ gilt. Also: $L(\sigma,\chi) \gtrsim_\varepsilon q^{-\varepsilon/2} - q^{-\varepsilon} \log^2(q) > 0$.

Somit gilt $\beta \leq 1 - q^{-1/(2A)}$, falls $q \geq q_0(A)$ gilt.

(Dabei ist $q_0(A)$ nicht effektiv in Abh. von A angebbar.)

- Wir ergänzen den Integrationsweg $[c-iT, c+iT]$ zur geschlossenen Kurve

$$\mathcal{C} = [c-iT, c+iT] \cup [c+iT, a+iT] \cup [a+iT, a-iT] \cup [a-iT, c-iT]$$

mit $a = 1 - \frac{c_2}{\log(x)}$, wo $c_2 = \min\{c_0, c_1\}$. Aus Lemma 10.7 folgt wie im

Beweis von Satz 10.8, dass auch für $\sigma = a$ und $|t| \leq 1$

die Abschätzung $\frac{L'}{L}(s,\chi) = O(\log^2(x))$ gilt.

Insgesamt erhalten wir mit $|\vartheta| \leq 2$, dass

$$\psi(x,\chi) = \operatorname{Res}_1\left(-\frac{L'}{L}(s,\chi)\frac{x^s}{s}\right) + \operatorname{Res}_\beta\left(-\frac{L'}{L}(s,\chi)\frac{x^s}{s}\right) + O_A\left(x \exp(-c\sqrt{\log(x)})\right)$$

$$= E(q,\chi)\, x - \vartheta x \exp(-\sqrt{\log(x)}) + O_A\left(x \exp(-c\sqrt{\log(x)})\right),$$

wobei der von β herrührende Term nur dann auftritt, falls β existiert.

$$\hookrightarrow -\frac{x^\beta}{\beta} = -\frac{x}{\beta} \cdot x^{\beta-1} \ll x \cdot e^{(\beta-1)\log(x)} \ll x e^{-\sqrt{\log(x)}},$$

denn $\beta - 1 \leq -q^{-1/(2A)} \leq -q^{-1/\left(2\frac{\log(q)}{\log\log(x)}\right)} = -e^{-\frac{\log\log(x)}{2}}$

$= -(\log(x))^{-1/2}$

Damit ist (i) gezeigt.

Zu (ii): Aus dem ONR folgt Satz 8.7, nach dem ist

$$\psi(x;q,a) = \sum_{\substack{n \leq x \\ n \equiv a (q)}} \Lambda(n) \overset{\downarrow}{=} \frac{1}{\varphi(q)} \sum_{\chi (q)} \overline{\chi}(a) \underbrace{\sum_{n \leq x} \chi(n) \Lambda(n)}_{= \psi(x,\chi)} \overset{(i)}{=} \underbrace{\frac{x}{\varphi(q)}}_{\text{für } \chi_0} + O_A\left(x \exp(-\tilde{c}\sqrt{\log(x)})\right).$$

anpassen

Zu (iii): Dies folgt aus (ii) durch partielle Summation, genau wie in Kor. 5.5. □

11.7. **Bem.:** Der im Beweis zu (i) auftretende Term $-\frac{x^\beta}{\beta}$, der nur bei Existenz von β vorkommt, zeigt auch (i)': $\Psi(x,\chi) = -\frac{x^\beta}{\beta} + O(x\cdot\exp(-c\sqrt{\log(x)}))$ für $\chi=\chi_\beta$,

(ii)' $\Psi(x;q,a) = \frac{x}{\varphi(q)} - \frac{\chi(a)}{\varphi(q)}\cdot\frac{x^\beta}{\beta} + O(x\cdot\exp(-c\sqrt{\log(x)}))$ für $\chi=\chi_\beta$,

[$\pi(x,q,a) \ll \frac{x}{q}$ ist trivial]

(iii)' $\pi(x;q,a) = \frac{li(x)}{\varphi(q)} - \frac{\chi(a)\,li(x^\beta)}{\varphi(q)} + O(x\cdot\exp(-c\sqrt{\log(x)}))$ für $\chi=\chi_\beta$, der Ausnahmecharakter zu β.

Dies gilt dann sogar für $q \le \exp(2c\sqrt{\log(x)})$.

11.8. **Bem.:** Siegel-Nullstellen treten nur selten auf: • Nach einem Satz von Landau ex. ein $c>0$ so, dass $\prod_{\chi(q)} L(s,\chi)$ höchstens eine Nst. β in $\sigma > 1-\frac{c}{\log(q)}$ hat. In diesem Fall ist β reell und der zugehörige Ausnahmecharakter ist reell.

• Nach einem Satz von Page ex. ein $c>0$ so, dass für alle $Q \ge 1$ die Fkt. $\prod_{q\le Q}\prod_{\chi(q)}{}^{*} L(s,\chi)$ höchstens eine Nst. β in $\sigma > 1-\frac{c}{\log(Qq)}$ hat.

Dabei durchläuft χ alle primitiven Charaktere mod q. [MV, 11.9, 11.10]

11.9. **Bem.:** Die gezeigte Absch. ⊛ im obigen Beweis von 11.6 zeigt, dass $\beta \le 1-\frac{c(\varepsilon)}{q^\varepsilon}$ für eine (ineffektive) Konstante $c(\varepsilon)>0$ ist, falls β ex. Auch diese Aussage wird gelegentlich als "Satz von Siegel" bezeichnet.

11.10. **Bem.:** Der Bereich $q \le \log^A(x)$ im Satz von Siegel-Walfisz fällt leider nur sehr klein aus. Die Konstante $A>0$ kann zwar bel. groß gewählt werden, aber die O_A-Konstante hängt in bislang nicht effektiv angebbarer Weise von A ab (wegen der Verwendung des Satzes von Siegel).

Jeder Satz, der im Beweis den Satz von Siegel-Walfisz (und damit den Satz von Siegel) benutzt, hat diesen Makel.

Das trifft z.B. zu auf den zentralen Satz von Bombieri-Vinogradov, den wir später in der Vorlesung beweisen werden.

11.11. **Bem.:** Die Anwendung der Perronschen Formel 3.12 auf $\Psi(x,\chi)$ unter Berücksichtigung aller überstrichenen Nullstellen von $L(s,\chi)$ und ihrer Residuen von $-\frac{L'}{L}(s,\chi)\frac{x^s}{s}$ führt auf explizite Formeln für $\Psi_0(x,\chi) := \frac{1}{2}(\Psi(x^+,\chi)-\Psi(x^-,\chi))$, nämlich $(x>1)$

$$\Psi_0(x,\chi) = -\sum_{\rho} \frac{x^\rho}{\rho} - \frac{1}{2}\log(x-1) - \frac{\chi(-1)}{2}\log(x+1) + C(\chi) \text{ mit } C(\chi) = \begin{cases} \frac{1}{1-\beta} + O(\log(q)), & \beta \text{ ex.}, \\ O(\log(q)), & \text{sonst.} \end{cases}$$

$\uparrow$ alle Nst. in $\mathrm{Re}\,\rho \ge 0$ inklusive ev. β

11.12. **Bem.:** (GRH) $\Rightarrow \Psi(x;\chi_0) = x + O(x^{1/2}\log^2(x))$, $\Psi(x;\chi) \ll x^{1/2}\log^2(x)$ für $\chi \ne \chi_0$ [MV, Cor. 12.11]

Somit: (GRH) $\Rightarrow \Psi(x;q,a) = \frac{x}{\varphi(q)} + O(x^{1/2}\log^2(x))$.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a12: Gaußsche Summen und $L(1,\chi)$

Stichworte: Formel für $L(1,\chi)$ mit $\tau_k(\chi)$, primitiver und induzierter Charakter, Formel für $L(1,\chi)$ mit geradem und ungeradem χ.

12.1. Einleitung: Der Wert $L(1,\chi)$ ist zahlentheoretisch interessant – aus verschiedenen Gründen. Hier zeigen wir mit Hilfe von Gauß-Summen eine explizite Formel dafür.

12.2. Vor.: Sei χ ein D.-Charakter mod q, $\chi \neq \chi_0$. Notation: $e(\alpha) := e^{2\pi i \alpha}$, $\alpha \in \mathbb{R}$.

12.3. Def.: $\tau_k(\chi) := \sum_{\substack{a (q) \\ (a,q)=1}} \chi(a)\, e\left(\frac{ak}{q}\right)$, wo $\tau_0(\chi) = \sum_{\substack{a(q) \\ (a,q)=1}} \chi(a) \overset{ONR}{=} 0$,

Bedingung entbehrlich, da $\chi(a)=0$ für $(a,q)>1$

heißt k-te Gaußsche Summe, mit $k \in \mathbb{Z}$.

12.4. Satz: Es ist $L(1,\chi) = -\frac{1}{q} \sum_{k=1}^{q-1} \tau_k(\chi) \log\left(1 - e\left(\frac{-k}{q}\right)\right)$.

Bew.: Für $j \in \mathbb{Z}$ ist (laut "ONR"

$$\frac{e(j)-1}{e(j/q)-1} = \frac{e(\frac{j}{q})^q - 1}{e(\frac{j}{q})-1} \overset{\text{geom. Summe}}{=} \sum_{k=0}^{q-1} e\left(\frac{jk}{q}\right) = \begin{cases} q, & q \mid j, \\ 0, & \text{sonst}, \end{cases} \quad (*)$$

also ist

für die in $\sigma>0$ holomorphe Fkt. $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \sum_{\substack{a(q) \\ (a,q)=1}} \sum_{n \equiv a(q)} \frac{\chi(a)}{n^s}$

$$= \sum_{\substack{a(q) \\ (a,q)=1}} \chi(a) \sum_{n\equiv a(q)} \frac{1}{n^s} \overset{(*)}{=} \sum_{\substack{a(q) \\ (a,q)=1}} \chi(a) \sum_{n\geq 1} \frac{1}{n^s} \cdot \frac{1}{q} \sum_{k=0}^{q-1} e\left(\frac{(a-n)k}{q}\right)$$

$$= \frac{1}{q} \sum_{k=0}^{q-1} \left(\sum_{\substack{a(q) \\ (a,q)=1}} \chi(a)\, e\left(\frac{ak}{q}\right)\right) \sum_{n\geq 1} \frac{1}{n^s} \cdot e\left(\frac{-nk}{q}\right) = \frac{1}{q} \sum_{k=1}^{q-1} \tau_k(\chi) \sum_{n\geq 1} \frac{e\left(-\frac{an}{q}\right)}{n^s}.$$

da $\tau_0(\chi)=0$.

Ist log der Hauptzweig der Logarithmusfunktion, so gilt für $|z|<1$:
$-\log(1-z) = \sum_{n\geq 1} \frac{z^n}{n}$. Mit dem Satz von Abel über die Werte von Potenzreihen auf dem Rand ihres Konvergenzkreises folgt:

$$\sum_{n\geq 1} \frac{e\left(\frac{-nk}{q}\right)}{n} = -\log\left(1 - e\left(\frac{-k}{q}\right)\right) \quad \text{für } 0<k<q$$

(vgl. z.B. AnZ 14.2, hier für $a_n = \frac{1}{n} e\left(\frac{-k}{q}\right)$ angewendet, da $\sum_{n\geq 1} \frac{e\left(\frac{-nk}{q}\right)}{n}$ kgt. [p.Z. und $(*)$] (bzw. Dirichlet-Krit.))

Daher folgt der Satz. $\square$

12.5. **Bem.:** Seien nun $d, q > 0$, $d \mid q$. Dann liefert die Projektion $\mathbb{Z}/q \twoheadrightarrow \mathbb{Z}/d \; (\hookrightarrow \mathbb{C}^\times)$ einen surjektiven Homomorphismus $\varrho : (\mathbb{Z}/q)^* \to (\mathbb{Z}/d)^*$.

⌜Denn ist $(k,d)=1$, $d = p_1^{e_1} \cdots p_s^{e_s}$, $q = d\, p_{s+1}^{f_{s+1}} \cdots p_t^{f_t}$ die PFZ, so wähle $k' \in \mathbb{Z}/q$ mit $k' \equiv \begin{cases} k & (p_1^{e_1}), \\ \vdots & \\ k & (p_s^{e_s}), \\ 1 & (p_i), \; s+1 \le i \le t \end{cases}$ laut CRS.

Dann ist $(k', q) = 1$, also $k' \in (\mathbb{Z}/q)^*$, und $\varrho(k') = k$.⌟

Wir erinnern an das Konzept eines primitiven Charakters, vgl. a 9.3.

12.6. **Def.:** (i) $\chi \in \mathrm{Hom}((\mathbb{Z}/q)^*, \mathbb{C}^*)$ heißt induziert von $\chi' \in \mathrm{Hom}((\mathbb{Z}/d)^*, \mathbb{C}^*)$, falls

$$\begin{tikzcd} (\mathbb{Z}/q)^* \arrow[r, "\chi"] \arrow[d, two heads, "\varrho"'] \arrow[dr, phantom, "="] & \mathbb{C}^* \\ (\mathbb{Z}/d)^* \arrow[ur, "\chi'"'] & \end{tikzcd}$$

gilt, d.h. wenn $\chi(a) = \begin{cases} \chi'(a), & \text{für } (a,q)=1, \\ 0, & \text{sonst.} \end{cases}$

(ii) $\chi \in \mathrm{Hom}((\mathbb{Z}/q)^*, \mathbb{C}^*)$ heißt primitiv, falls gilt:
$\forall d \mid q, d \neq q \;\; \forall \chi' \in \mathrm{Hom}((\mathbb{Z}/d)^*, \mathbb{C}^*)$: χ ist nicht von χ' induziert,
d.h. wenn q die kleinste Periode von $\chi : \mathbb{Z} \to \mathbb{C}$ ist.

12.7. **Bsp.:** Hier ist χ mod 10 von einem primitiven χ_1 mod 5 induziert:

$n(10)$	1	2	3	4	5	6	7	8	9	10
$\chi_1(n)$	1	i	$-i$	-1	0	1	i	$-i$	-1	0
$\chi(n)$	1	0	$-i$	0	0	0	i	0	-1	0

12.8. **Lemma:** Sei χ primitiver Charakter mod q, $0 \le k < q$. Dann gilt:

$$\tau_k(\chi) = \begin{cases} \overline{\chi}(k)\, \tau_1(\chi), & \text{falls } (k,q)=1, \\ 0, & \text{sonst.} \end{cases}$$

Bew.: • Sei $(k,q)=1$ und $l \in \mathbb{Z}$ mit $lk \equiv 1 (q)$. Dann ist

$$\tau_k(\chi) = \sum_{a(q)} \chi(a)\, e\!\left(\frac{ak}{q}\right) = \sum_{a(q)} \chi(al)\, e\!\left(\frac{alk}{q}\right) = \chi(l) \sum_{a(q)} \chi(a)\, e\!\left(\frac{a}{q}\right)$$
$$= \chi(l)\, \tau_1(\chi) = \overline{\chi}(k)\, \tau_1(\chi), \text{ da } \overline{\chi}(k) = \chi(k)^{-1} = \chi(l).$$

• Sei $(k,q) \neq 1$, d.h. $\mathrm{Ann}(\overline{k}) = \{\underline{m} \in \mathbb{Z}/q \,;\, \underline{m} \cdot \underline{k} = \underline{0}\} = \langle \underline{d} \rangle \neq \{\underline{0}\}$. $\leftarrow dk \equiv 0 (q)$

Da χ primitiv ist, ex. ein $\underline{b} \in \ker(\varrho : (\mathbb{Z}/q)^* \to (\mathbb{Z}/d)^*) = 1 + (\underline{d})$ mit $\chi(\underline{b}) \neq 1$.

⌜Sonst ist χ induziert von χ' nach Hom.satz:

$$\begin{tikzcd} (\mathbb{Z}/q)^* \arrow[r, "\chi"] \arrow[d, two heads, "\varrho"'] \arrow[dr, phantom, "="] & \mathbb{C}^* \\ (\mathbb{Z}/d)^* \arrow[ur, dashed, "\chi'"'] & \end{tikzcd}$$

χ', ex. eind. falls $\ker \varrho = \ker \chi$.⌟

Es folgt: $\tau_k(\chi) = \sum_{a(q)} \chi(a)\, e\!\left(\frac{ak}{q}\right) = \sum_{a(q)} \chi(a)\, e\!\left(\frac{ak}{q}\right)$

$$= \sum_{a(q)} \chi(ab)\, e\!\left(\frac{abk}{q}\right) \underset{\substack{b = 1 + sd \\ \Rightarrow \underline{b}\,\underline{k} = \underline{k} \leftarrow \text{mod } q}}{=} \chi(b) \sum_{a(q)} \chi(a)\, e\!\left(\frac{ak}{q}\right) = \underbrace{\chi(b)}_{\neq 1}\, \tau_k(\chi),$$

also ist $\tau_k(\chi) = 0$. □

$\chi(-1)$ ist 2-te EW, da $\chi^2(-1) = \chi((-1)^2) = 1$

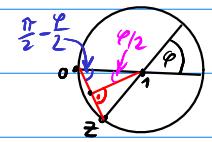
12.9. Satz: Sei χ ein primitiver Charakter mod $q > 1$. Dann gilt:

$$L(1,\chi) = \begin{cases} -\dfrac{\tau_1(\chi)}{q} \displaystyle\sum_{0<k<q} \bar\chi(k) \log \sin\left(\frac{k\pi}{q}\right), & \text{falls } \chi \text{ gerade, d.h. } \chi(-1)=1, \\[2ex] \dfrac{\tau_1(\chi)\pi i}{q^2} \displaystyle\sum_{0<k<q} \bar\chi(k)\, k, & \text{falls } \chi \text{ ungerade, d.h. } \chi(-1)=-1. \end{cases}$$

Bew.: Für $z = re^{i\psi} \in \mathbb{C}$ mit $-\pi < \psi < \pi$ gilt $\log z = \log r + \psi i$.

Für $k \in \mathbb{N}$ setze $\varphi := \frac{2\pi}{q} k$, $z := 1 - \omega^k$, $\omega := e\left(\frac{1}{q}\right)$.

Dann ist $z = 2\sin\left(\frac{\varphi}{2}\right) e^{-i(\pi-\varphi)/2}$ laut Skizze. $\left[\sin\left(\frac{\varphi}{2}\right) = \frac{|z|/2}{1}\right]$



Nun ist $\frac{\pi}{2} - \frac{\varphi}{2} = \frac{\pi}{2} - \frac{\pi k}{q} = \left(\frac{1}{2} - \frac{k}{q}\right)\pi$.

Es folgt: $\log(1-\omega^k) = \log(2) + \log\sin\left(\frac{\varphi}{2}\right) + \left(\frac{k}{q} - \frac{1}{2}\right)\pi i$.

Somit ist nach 12.4:

$$L(1,\chi) = -\frac{1}{q} \sum_{0<k<q} \tau_k(\chi) \log(1-\omega^{-k}) \overset{12.8}{=} -\frac{\tau_1(\chi)}{q} \sum_{0<k<q} \bar\chi(k) \log(1-\omega^{-k})$$

$$= -\frac{\tau_1(\chi)}{q} \sum_{0<k<q} \underbrace{\bar\chi(-k)}_{\bar\chi(-1)\bar\chi(k)} \log(1-\omega^k) = -\frac{\chi(-1)\tau_1(\chi)}{q} \sum_{0<k<q} \bar\chi(k) \log(1-\omega^k)$$

$$= -\frac{\chi(-1)\tau_1(\chi)}{q} \sum_{0<k<q} \bar\chi(k)\left(\log\sin\left(\frac{k\pi}{q}\right) + \frac{k}{q}\pi i\right), \quad \text{da } \sum_{0<k<q} \bar\chi(k) = 0.$$

$\rightsquigarrow$ Terme ohne k fallen raus

- Falls χ gerade, d.h. $\chi(-1)=1$, ist

$$\sum_{0<k<q} \bar\chi(k)\, k = \sum_{0<k<q} \underbrace{\bar\chi(q-k)}_{=\bar\chi(-k)=\bar\chi(k)} (q-k) = -\sum_{0<k<q} \bar\chi(k)\, k,$$

da $\left(\sum_{0<k<q} \bar\chi(k)\right) q \overset{\text{ONR}}{=} 0$

also ist $\sum_{0<k<q} \bar\chi(k)\, k = 0$ und somit $L(1,\chi) = -\frac{\tau_1(\chi)}{q} \sum_{0<k<q} \bar\chi(k) \log\sin\left(\frac{k\pi}{q}\right)$.

- Falls χ ungerade, d.h. $\chi(-1)=-1$, ist

$$\sum_{0<k<q} \bar\chi(k) \log\sin\left(\frac{k\pi}{q}\right) = \sum_{0<k<q} \underbrace{\bar\chi(q-k)}_{=-\bar\chi(k)} \log \underbrace{\sin\left(\pi - \frac{k\pi}{q}\right)}_{=\sin\left(\frac{k\pi}{q}\right)}$$

$$= -\sum_{0<k<q} \bar\chi(k) \log\sin\left(\frac{k\pi}{q}\right), \text{ also ist } \sum_{0<k<q} \bar\chi(k) \log\sin\left(\frac{k\pi}{q}\right) = 0.$$

Somit ist $L(1,\chi) = \frac{\tau_1(\chi)}{q} \sum_{0<k<q} \bar\chi(k) \frac{k}{q} \pi i = \frac{\tau_1(\chi)\pi i}{q^2} \sum_{0<k<q} \bar\chi(k)\, k.$ $\square$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a13: Vorzeichen bei Gaußschen Summen

Stichworte: $|\tau_1(\chi)| = \sqrt{q}$ für primitive χ mod q, Satz von Gauß über den Wert von $\tau_1(\chi)$ im Fall eines primitiven quadratischen Charakters; Beweis nach Schur

---

13.1. Einleitung: Sehr leicht ergibt sich $|\tau_1(\chi)| = \sqrt{q}$ für primitives χ mod q. Ist χ mod p primitiv und quadratisch, zeigen wir $\tau_1(\chi) = \sqrt{p}$, falls χ gerade,
und $\tau_1(\chi) = i\sqrt{p}$, falls χ ungerade.

13.2. Def.: Ein Gruppencharakter χ heißt quadratisch, falls $\chi^2 = 1$, d.h. falls $\operatorname{im}\chi \subseteq \{\pm 1\}$. (Auch: reell, Gegenteil: imaginär/nichtreell).

13.3. Bem.: Der Charakter eines quadratischen Zahlkörpers ist quadratisch (s. a15.7).

13.4. Lemma: Für primitive Charaktere χ mod q gilt: $|\tau_1(\chi)| = \sqrt{q}$.

Bew.: Es ist $|\tau_1(\chi)|^2 = \tau_1(\chi)\overline{\tau_1(\chi)} = \sum_{a(q)} \chi(a)\omega^a \sum_{b(q)} \overline{\chi(b)}\,\omega^{-b}$

$$= \sum_{a,b(q)} \chi(a)\bar{\chi}(b)\,\omega^{a-b} = \sum_{b,c(q)} \underbrace{\chi(bc)\bar{\chi}(b)}_{=\chi(c) \text{ falls } (b,q)=1} \omega^{b(c-1)}$$

$$\overset{(*)}{=} \sum_{\substack{b=0 \\ \cancel{(b,q)=1}}}^{q-1} \sum_{c(q)} \chi(c)\,\omega^{b(c-1)} = \sum_{c(q)} \chi(c) \underbrace{\sum_{b=0}^{q-1} \omega^{(c-1)b}}_{=\begin{cases} q, & c=1, \\ 0, & \text{sonst} \end{cases}} = \chi(1)\cdot q = q.$$

In (*) wird benutzt: Falls $(b,q)>1$, ist

$$\sum_{c(q)} \chi(c)\,\omega^{(c-1)b} = \omega^{-b} \sum_{c(q)} \chi(c)\,\omega^{cb} = \omega^{-b}\tau_b(\chi) \overset{12.8}{=} 0. \qquad \square$$

13.5. Satz (Gauß): Sei $q > 2$ und χ ein primitiver quadratischer Charakter mod q. Dann gilt für die normierte Gaußsche Summe

$$\tau(\chi) := \tau_1(\chi) = \begin{cases} \sqrt{q}, & \chi \text{ gerade}, \\ i\sqrt{q}, & \chi \text{ ungerade}. \end{cases}$$

13.6. **Bew.:** • Nur für $q>2$ prim, der allg. Fall wird darauf zurückgeführt.
⌈S. z.B. [Montgomery/Vaughan: Multiplicative NT, Theorem 9.17]⌋

• Für $p>2$ prim gibt es genau einen nichttrivialen quadratischen Charakter mod p, nämlich $\chi(k)=\left(\frac{k}{p}\right)$. ⌈Denn $\chi: \mathbb{F}_p^\times \to \{\pm 1\}$ hat Kern vom Index 2 in $\mathbb{F}_p^\times$, dieser ist also $(\mathbb{F}_p^\times)^2$ und ist eindeutig.⌋

Sei $\omega := e^{\frac{2\pi i}{p}}$. Somit ist $\tau(\chi)=\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\omega^k$, wissen nach 13.4: $\tau(\chi)\overline{\tau(\chi)}=p$.

Nun ist $\overline{\tau(\chi)}=\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\omega^{-k}=\sum_{k=1}^{p-1}\left(\frac{-k}{p}\right)\omega^k=\underbrace{\left(\frac{-1}{p}\right)}_{=\pm 1}\tau(\chi)$,

also ist $\tau(\chi)=\begin{cases}\pm\sqrt{p}, & \text{falls } p\equiv 1\ (4),\\ \pm i\sqrt{p}, & \text{falls } p\equiv 3\ (4).\end{cases}$

• Bestimmung des Vorzeichens (nach Schur):

Es ist $\tau(\chi)=\sum_{k\in(\mathbb{F}_p^\times)^2}\omega^k-\sum_{k\in\mathbb{F}_p^\times\setminus(\mathbb{F}_p^\times)^2}\omega^k$. Wegen $\sum_{k=0}^{p-1}\omega^k=0$

gilt $-\sum_{k\in\mathbb{F}_p^\times\setminus(\mathbb{F}_p^\times)^2}\omega^k=1+\sum_{k\in(\mathbb{F}_p^\times)^2}\omega^k$, und somit $\tau(\chi)=1+2\sum_{k\in(\mathbb{F}_p^\times)^2}\omega^k=\sum_{k=0}^{p-1}\omega^{k^2}$.

Dies ist die Spur der Vandermonde-Matrix $A:=(\omega^{jk})_{0\le j,k<p}$.

13.7. **Zwischenbem.:** Für jede $p\times p$-Matrix A gilt: $T^2 I_p - A^2=(TI_p-A)(TI_p+A)$,

also folgt $f_{A^2}(T^2):=\det(T^2I_p-A^2)=f_A(T)\cdot(-1)^p\det(-TI_p-A)$
$=f_A(T)\cdot(-1)^p f_A(-T)$.

Falls $f_{A^2}(T)=\prod_i(T-\mu_i)$, $f_A(T)=\prod_j(T-\lambda_j)$, so folgt also
$\prod_i(T^2-\mu_i)=\prod_j(T-\lambda_j)(T+\lambda_j)=\prod_j(T^2-\lambda_j^2)$, also ist $\mu_i=\lambda_j^2$.

13.8. **Fortsetzung von 13.6:** Seien $\lambda_1,\dots,\lambda_p$ die EWe von $A=(\omega^{jk})_{0\le j,k<p}$.

Dann gilt $\tau(\chi)=\lambda_1+\dots+\lambda_p$, sowie:

$$A^2=\begin{pmatrix} p & 0 & \cdots & 0\\ 0 & 0 & \cdots\ 0 & p\\ \vdots & \vdots & \iddots & 0\\ 0 & p & 0\ \cdots & 0\end{pmatrix}$$

⌈da $\sum_{i=0}^{p-1}\omega^{jl+lk}=\sum_{l=0}^{p-1}\omega^{(j+k)l}$
$=\begin{cases}p, & j+k\equiv 0\ (p),\\ 0, & \text{sonst.}\end{cases}$⌋

Die bezüglich der Standardbasis durch A^2 definierte lin. Abb. ist

$$\begin{aligned} e_0 &\mapsto p e_0 \\ e_1 &\mapsto p e_{p-1} \\ e_2 &\mapsto p e_{p-2} \\ &\vdots \\ e_{p-1} &\mapsto p e_1 \end{aligned}$$

Bezüglich der Basis $e_0, e_1, e_{p-1}, e_2, e_{p-2}, \dots$ ist die Matrix dieser lin. Abb.

also $\begin{pmatrix} p & & & & & 0 \\ & 0 & p & & & \\ & p & 0 & & & \\ & & & 0 & p & \\ & & & p & 0 & \\ 0 & & & & & \ddots \end{pmatrix}$.

Somit ist

$$f_{A^2}(T) = (T-p)(T^2-p^2)^{\frac{p-1}{2}} = (T-p)^{\frac{p+1}{2}}(T+p)^{\frac{p-1}{2}}.$$

Sei also OE $\lambda_1^2 = \dots = \lambda_{\frac{p+1}{2}}^2 = p$ und $\lambda_{\frac{p+3}{2}}^2 = \dots = \lambda_p^2 = -p$.

Weiter sei

$$a := \#\{j;\ \lambda_j = \sqrt{p}\},\quad b := \#\{j;\ \lambda_j = -\sqrt{p}\},$$
$$c := \#\{j;\ \lambda_j = i\sqrt{p}\},\quad d := \#\{j;\ \lambda_j = -i\sqrt{p}\}.$$

Somit ist $\tau(X) = ((a-b)+(c-d)i)\sqrt{p}$, wo $\sqrt{p} > 0$.

Weiter gilt: (0) $a+b = \frac{p+1}{2}$ und $c+d = \frac{p-1}{2}$,

(1) $\begin{cases} a-b = \pm 1 \text{ und } c = d, & \text{falls } p \equiv 1\ (4), \\ a = b \text{ und } c-d = \pm 1, & \text{falls } p \equiv 3\ (4), \end{cases}$ da ja $\tau(X) = \begin{cases} \pm\sqrt{p}, & p \equiv 1\ (4), \\ \pm i\sqrt{p}, & p \equiv 3\ (4). \end{cases}$

Aus $\det(A^2) = (-1)^{\frac{p-1}{2}} p^p = (-1)^{p\cdot\frac{p-1}{2}} p^p$ folgt: $\det A = \pm i^{p\cdot\frac{p-1}{2}} p^{\frac{p}{2}}$.

Setzen nun $\zeta := e^{\pi i/p} = \cos\frac{\pi}{p} + i\sin\frac{\pi}{p} \in \mathbb{C}$.

Dann ist $\det A \underset{\text{Vandermonde}}{=} \prod_{0\le r<s<p} (\omega^s - \omega^r) = \prod_{0\le r<s<p} \zeta^{r+s}(\zeta^{s-r} - \zeta^{-(s-r)})$

$$= \Big(\prod_{0\le r<s<p} \zeta^{r+s}\Big)\cdot\Big(\prod_{0\le r<s<p} 2i\sin\frac{(s-r)\pi}{p}\Big) = 1\cdot i^{p\cdot\frac{p-1}{2}}\cdot \underbrace{2^{p\cdot\frac{p-1}{2}}}_{>0}\cdot \underbrace{\prod_{0\le r<s<p}\sin\frac{(s-r)\pi}{p}}_{>0},$$

da $\Big(\sum_{0\le r<s<p}(r+s) \underset{13.9}{=} 2p\left(\frac{p-1}{2}\right)^2$ teilbar durch $2p\Big)$ und da $\left(\#\{(r,s)\in\{0,\dots,p-1\}^2;\ r<s\} = p\cdot\frac{p-1}{2}\right)$ nach 13.10.

Der Vergleich der beiden Ausdrücke für $\det A$ liefert (VZ+!)

$$\det A = i^{p\cdot\frac{p-1}{2}} p^{\frac{p}{2}} = \prod_{j=1}^{p}\lambda_j = (-1)^b i^{(c-d)} p^{\frac{p}{2}} = i^{(2b+c-d)} p^{p/2},$$

$\ulcorner (-i)^d = (i^3)^d = i^{4d-d} = i^{-d} \lrcorner$ $\quad$ ⊗, s. unten

also ist $2b+c-d \equiv p\cdot\frac{p-1}{2}\ (4)$.

Mit (0) und (1) folgt:

$\rightsquigarrow p \equiv 1\,(4)$: $a-b \underset{(0)}{=} \frac{p+1}{2} - 2b \underset{\substack{(1)\\(c=d)\\ \text{aus } \otimes}}{\equiv} \frac{p+1}{2} - \frac{p-1}{2} \cdot \underbrace{p}_{\equiv 1(4)} \;(4) \equiv 1\;(4).$

$\rightsquigarrow p \equiv 3\,(4)$: $c-d \underset{\otimes}{\equiv} \underbrace{p}_{\equiv -1(4)} \cdot \frac{p-1}{2} - \underbrace{2b}_{\substack{a+b\\ \text{nach } (1)}} \overset{(0)}{\equiv} -\frac{p-1}{2} - \frac{p+1}{2} \equiv -p \equiv 1\;(4).$

In beiden Fällen folgt mit (1): $a-b=1$ bzw. $c-d=1$.

Somit ist $\tau(\chi) = ((a-b)+(c-d)i)\sqrt{p} = \begin{cases} \sqrt{p}, & p \equiv 1\,(4), \\ i\sqrt{p}, & p \equiv 3\,(4). \end{cases}$ Also: $\tau(\chi) = \begin{cases} \sqrt{p}, & \chi \text{ gerade}, \\ i\sqrt{p}, & \chi \text{ ungerade}. \end{cases}$ □

13.9. Beh.: Für p prim gilt $\sum_{0 \le r < s < p} (r+s) = 2p\left(\frac{p-1}{2}\right)^2$.

Bew.:

$$\text{l.S.} = \sum_{0 \le r < s \le p-1} r + \sum_{0 \le r < s \le p-1} s = \sum_{0 \le s \le p-1} \underbrace{\sum_{r=0}^{s-1} r}_{= s(s-1)/2} + \sum_{0 \le s \le p-1} s \underbrace{\sum_{r=0}^{s-1} 1}_{=s}$$

$$= \sum_{0 \le s \le p-1} \left(s\frac{s-1}{2} + s^2\right) = \frac{3}{2}\sum_{s=0}^{p-1} s^2 - \frac{1}{2}\sum_{s=0}^{p-1} s = \frac{3}{2} \cdot \frac{p}{6} \cdot (p-1) \cdot (2p-1) - \frac{1}{4} \cdot (p-1)p$$

$$\left[\sum_{k=1}^{n} k^2 = \frac{1}{6} n (n+1)(2n+1)\right]$$

$$= p \cdot \left(\frac{p-1}{2} \cdot \frac{2p-1}{2} - \frac{p-1}{4}\right) = p \cdot \frac{p-1}{2} \cdot \underbrace{\left(\frac{2p-1}{2} - \frac{1}{2}\right)}_{= p-1 = 2 \cdot \frac{p-1}{2}} = \text{r.S.} \checkmark$$

□

13.10. Beh.: Für p prim gilt $\#\{(r,s) \in \{0,\dots,p-1\}^2 ; r<s\} = p \cdot \frac{p-1}{2}$.

Bew.: $\text{l.S.} = \sum_{0 \le r < s \le p-1} 1 = \sum_{0 \le s \le p-1} \sum_{r=0}^{s-1} 1 = \sum_{0 \le s \le p-1} s = \frac{1}{2} p (p-1).$ ✓

□

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a14: Verteilung der Ideale in Zahlringen

Stichworte: Zählfunktion der Ideale mit Norm $\leq \lambda$ in einer Idealklasse eines ZKs, asymptotische Formel $\sim \kappa \cdot \lambda$, Berechnung von κ im Fall eines quadratischen ZKs

---

14.1. Einleitung: Wir zeigen für die Anzahl der ganzen Ideale einer Idealklasse mit Norm $\leq \lambda$ eine asymptotische Formel der Form $\kappa\lambda + O(\lambda^{1-1/n})$, wobei im Fall $n=2$ die Konstante κ genau in Abhängigkeit der Diskriminante (und der Grundeinheit u für $K \subseteq \mathbb{R}$) berechnet werden kann.

14.2. Voraussetzung: Sei K ein ZK vom Grad n mit Zahlring A, $C \in \mathcal{C}(K)$.
Für $\lambda \geq 0$ sei $i(\lambda) := \#\{\mathfrak{a} \subseteq A;\ \mathfrak{a} \text{ Ideal},\ N(\mathfrak{a}) \leq \lambda\}$,
sowie $i_C(\lambda) := \#\{\mathfrak{a} \subseteq A;\ \mathfrak{a} \text{ Ideal},\ \mathfrak{a} \in C,\ N(\mathfrak{a}) \leq \lambda\}$.
Es ist $i(\lambda) = \sum_{C \in \mathcal{C}(K)} i_C(\lambda)$.

14.3. Satz: Es gibt ein $\kappa \geq 0$ so, dass für alle $C \in \mathcal{C}(K)$ gilt:
$$i_C(\lambda) = \kappa\lambda + \varepsilon_C(\lambda) \quad \text{mit} \quad \varepsilon_C(\lambda) = O(\lambda^{1-1/n}) \qquad (\text{für } \lambda \to \infty).$$

Im Fall $n=2$ (quadratisches ZK) gilt:
(i) $\kappa = \dfrac{2\pi}{\#(A^\times)\cdot\sqrt{|\mathrm{disc}(K)|}}$, falls $\mathrm{disc}(K) < 0$, d.h. wenn K imaginär-quadr.
(ii) $\kappa = \dfrac{2\log(u)}{\sqrt{\mathrm{disc}(K)}}$, falls $\mathrm{disc}(K) > 0$, und $u > 1$ die Grundeinheit, d.h. wenn K reellquadratisch.

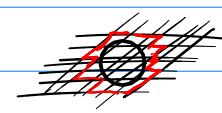
Bew.: (nur $n=2$)
Sei $\mathfrak{b} \in C^{-1}$ ein ganzes Ideal. Haben Bijektionen
$$\{\mathfrak{a} \in C;\ N(\mathfrak{a}) \leq \lambda\} \longleftrightarrow \{(x);\ 0 \neq x \in \mathfrak{b};\ N((x)) \leq \lambda N(\mathfrak{b})\} =: \mathcal{H}$$
vermöge
$$\mathfrak{a} \longmapsto \mathfrak{a}\cdot\mathfrak{b}$$
und
$$(x)\cdot\mathfrak{b}^{-1} \longleftarrow\!\shortmid (x).$$
[Denn: $\mathfrak{a}\cdot\mathfrak{b} = (x)$, und $N(\mathfrak{a})\cdot N(\mathfrak{b}) = N((x)) \leq \lambda N(\mathfrak{b})$.]
Zählen nun die Elemente rechts in $\mathcal{H}$.

(i): Sei K imaginär quadratisch. Dann ist $U := A^\times$ endlich und $i_c(\lambda) = \frac{1}{\#U} \cdot \#\{x \in \mathfrak{o} \setminus \{0\};\ |N(x)| \le \lambda N(\mathfrak{o})\}$.

⌜Denn: $(x) = (y) \Leftrightarrow x, y$ in derselben U-Bahn von $U \times (\mathfrak{o} \setminus \{0\}) \to (\mathfrak{o} \setminus \{0\})$, $(u, x) \mapsto ux$. ⌟

Sei $\sigma : K \hookrightarrow \mathbb{C} = \mathbb{R} \times \mathbb{R}$, $x \mapsto x = (\operatorname{Re} x, \operatorname{Im} x)$ die kanonische Einbettung.
Es ist $N(x) = |x|^2$, und $\mathfrak{o} = \sigma\mathfrak{o}$ ist ein Gitter in $\mathbb{R} \times \mathbb{R}$ mit
$\gamma := \operatorname{vol}(\mathbb{R}^2/\mathfrak{o}) = \frac{1}{2}\sqrt{|\operatorname{disc}(K)|} \cdot N(\mathfrak{o})$ nach Z16.12 aus ZT I.
Für $\varrho \ge 0$ sei $S(\varrho) := \{x \in \mathbb{C};\ |x| \le \varrho\}$, G eine Grundmasche des Gitters $\mathfrak{o}$ und δ die Länge der langen Diagonalen von G.
Sei nun $n(\varrho) := \#\{x \in \mathfrak{o};\ |x| \le \varrho\}$,
$n_-(\varrho) := \#\{x \in \mathfrak{o};\ (x + G) \subseteq S(\varrho)\}$
$n_+(\varrho) := \#\{x \in \mathfrak{o};\ (x + G) \cap S(\varrho) \ne \emptyset\}$.

Es gilt $n_-(\varrho) \le n(\varrho) \le n_+(\varrho)$ und
$$\pi(\varrho - \delta)^2 \le n_-(\varrho) \cdot \gamma \le \pi\varrho^2 \le n_+(\varrho)\gamma \le \pi(\varrho + \delta)^2.$$



Sei nun $\varrho := \sqrt{\lambda N(\mathfrak{o})}$. Dann folgt:
$$-2\pi\varrho\delta + \pi\delta^2 \le n_-(\varrho) \cdot \gamma - \pi\varrho^2 \le n(\varrho)\gamma - \pi\varrho^2 \le n_+(\varrho)\gamma - \pi\varrho^2 \le 2\pi\varrho\delta + \pi\delta^2,$$
also $\left| n(\varrho) - \frac{\pi\varrho^2}{\gamma} \right| \le \frac{2\pi\varrho\delta + \pi\delta^2}{\gamma}$ $(= O(\lambda^{1/2}))$,
somit:
$$n(\sqrt{\lambda N(\mathfrak{o})}) = \frac{\pi\lambda}{\gamma} N(\mathfrak{o}) + O(\lambda^{1/2}) = \frac{2\pi\lambda}{\sqrt{|\operatorname{disc}(K)|}} + O(\lambda^{1/2}).$$
Daher: $i_c(\lambda) = \frac{2\pi}{(\#A^\times) \cdot \sqrt{|\operatorname{disc}(K)|}} \lambda + O(\lambda^{1/2})$.

(ii): Sei K reellquadratisch. Dann ist $K = \mathbb{Q}(\sqrt{m})$ mit $m > 1$ und $A^\times = \{\pm 1\} \times U$, wo $U = \langle u \rangle$ unendl. zyklisch, $u > 1$ die Grundeinheit.
Nun operiert U auf $\mathfrak{o} \setminus \{0\}$ vermöge Multiplikation, d.h. mit
$$U \times (\mathfrak{o} \setminus \{0\}) \to \mathfrak{o} \setminus \{0\},\ (u, x) \mapsto ux.$$
Ist nun $Y \subseteq (\mathfrak{o} \setminus \{0\})$ ein Repräsentantensystem für die U-Bahnen, so gilt: $i_c(\lambda) = \frac{1}{2} \#\{x \in Y;\ |N(x)| \le \lambda N(\mathfrak{o})\}$.
↑ für $\{\pm 1\}$

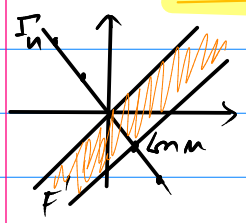
Haben die kanonische Einbettung $\sigma: K \hookrightarrow \mathbb{R}\times\mathbb{R}$, $x \mapsto (\sigma_1 x, \sigma_2 x)$, betr. die Abb.

$$\mathrm{Ln}: (A\setminus\{0\}) \subseteq K^\times \xrightarrow{\sigma|_{K^\times}} \mathbb{R}^\times\times\mathbb{R}^\times \xrightarrow{\ln} \mathbb{R}\times\mathbb{R},$$
$$x \longmapsto (\sigma_1 x, \sigma_2 x) \longmapsto (\log|\sigma_1 x|, \log|\sigma_2 x|).$$

Dann ist $\mathrm{Ln}|_U$ ein Isomorphismus von U auf ein Gitter Γ_U mit $\Gamma_U \subseteq H := \{(y_1,y_2)\in\mathbb{R}\oplus\mathbb{R};\ y_1+y_2=0\}$.

Denn: $A^\times \xrightarrow{\mathrm{Ln}} \mathbb{R}\times\mathbb{R}$ hat Kern $\{\pm 1\}$, und $\mathrm{Ln}(U^\times) = \Gamma_U \subseteq \{\sum x_i + 2\sum y_i = 0\}$ ⌜$1 = \prod|x_i|\prod|y_i|^2$⌟

Es ist $\Gamma_U := \mathbb{Z}\cdot\mathrm{Ln}(u)$,



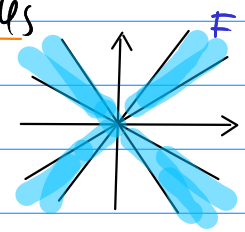
wo $\mathrm{Ln}(u) = (\log(u), -\log(u))$.

Sei $F' := \{a(1,1) + b\,\mathrm{Ln}\,u;\ a\in\mathbb{R},\ 0\le b<1\}$, dies ist ein Repräsentantensystem für $\mathbb{R}\oplus\mathbb{R}/\Gamma_U$. Mit Lemma 14.4 ist $F := (\mathrm{Ln})^{-1}(F')$ ein Repräsentantensystem für $\mathbb{R}^\times\times\mathbb{R}^\times/\sigma U$, also $F := \{(\pm e^a u^b, \pm e^a (\frac{1}{u})^b);\ a\in\mathbb{R}, 0\le b<1\}$.

F heißt Fundamentalbereich von K. Sei nun $X := \sigma(\mathfrak{o}\setminus\{0\})\cap F$, dann ist X ein Repräsentantensystem für die $\sigma(U)$-Bahnen, in die $\sigma(\mathfrak{o}\setminus\{0\})$ zerfällt. Also: $i_C(\lambda) = \frac{1}{2} n(\lambda\cdot N(\mathfrak{o}))$,

wobei für $\rho>0$ dann $n(\rho)$ zu setzen ist als

$n(\rho) := \#\{(x_1,x_2)\in X;\ |x_1|\cdot|x_2|\le\rho\} = \#$ Punkte $(x_1,x_2)\neq(0,0)$ des Gitters $\sigma\mathfrak{o}$ mit $(x_1,x_2)\in F$ und $|x_1|\cdot|x_2|\le\rho$.

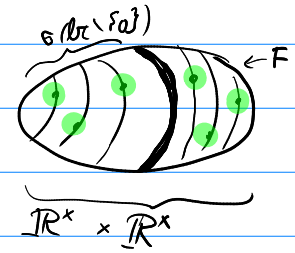


Sei $v(\rho) := \mu(F\cap\{(x_1,x_2)\in\mathbb{R}_{\ge0}\times\mathbb{R}_{\ge0};\ x_1x_2\le\rho\})$.

Ähnlich wie in (i) folgt: $n(\rho) = \underbrace{4}_{\#\text{Quadranten}}\cdot\frac{v(\rho)}{\sigma} + O(\sqrt{\rho})$,

wobei $\sigma = \mathrm{vol}(\mathbb{R}^2/\sigma\mathfrak{o}) = \sqrt{\mathrm{disc}(K)}\cdot N(\mathfrak{o})$. Die Dreiecke $\Delta(0,\sqrt{\rho},(\sqrt{\rho},\sqrt{\rho}))$ und $\Delta(0,\sqrt{\rho}u,(\sqrt{\rho}u,\sqrt{\rho}\frac{1}{u}))$ haben dieselbe Fläche, es folgt:

$$v(\rho) = \int_{\sqrt{\rho}}^{\sqrt{\rho}u} \frac{\rho}{x}\,dx = \rho(\log(\sqrt{\rho}\,u) - \log(\sqrt{\rho})) = \rho\log(u).$$



Somit ist $i_C(\lambda) = \frac{2\log(u)}{\sqrt{\mathrm{disc}(K)}}\cdot\lambda + O(\lambda^{1/2})$. □

14.4. Lemma: Sei $f: G\to G'$ Hom. abelscher Gruppen, $H\le G$ UG mit $H\cap\ker(f)=\{e\}$. Sei $X'\subseteq G'$ ein Repräsentantensystem für $G'/f(H)$. Dann ist $X = f^{-1}(X')$ ein Repräsentantensystem für G/H. ⌜o. Bew.⌟

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a15: Die Dedekindsche ζ-Funktion

Stichworte: Zählfunktion der Ideale von Norm n, Dedekindsche ζ-Fkt. von K, Formel für hk mit ζ_K, Eulerproduktdarstellung von ζ_K, Charakter χ eines quadratischen ZKs, Formel $hk = L(1,\chi)$ im Fall eines quadratischen ZKs

---

15.1. Einleitung: Damit wir analytische Methoden in Fragestellungen zur Klassenzahl einsetzen können, definieren wir die Dedekindsche ζ-Funktion ζ_K mit der Zählfunktion der Ideale von Norm n, welche aufgrund der in a14 gezeigten Asymptotiken (absolut) konvergiert. Die Entwicklung in ein Eulerprodukt zeigt im Fall des quadratischen ZKs K, dass $\zeta_K(s) = \zeta(s)\cdot L(s,\chi)$ ist, wo χ der Charakter von K ist.
Um $i(\lambda)$ besser zu verstehen, betr. wir die Zählfkt. der Ideale mit Norm n.

15.2. Def.: Sei K ein ZK mit ZR A. Für $n \geq 1$ sei
$$j_n := \#\{\mathfrak{a} \subseteq A;\ \mathfrak{a} \text{ Ideal}, N(\mathfrak{a}) = n\}.$$
Für $\operatorname{Re} s > 1$ setze $\zeta_K(s) := L(K,s) := \sum_{n\geq 1} \frac{j_n}{n^s}$.
Erinnerung: Die Norm $N(\mathfrak{a})$ war def. als
$$N(\mathfrak{a}) := \#A/\mathfrak{a}.$$
Die Fkt. ζ_K heißt Dedekindsche ζ-Fkt. von K.

15.3. Bem.: (1) Es ist $\sum_{n\leq\lambda} j_n = O(\lambda)$ nach 14.3. Es folgt Konvergenz für $\operatorname{Re} s > 1$.
(2) Es ist $j_n = \sum_{\substack{\mathfrak{a},\\ N(\mathfrak{a})=n}} 1$, also $\zeta_K(s) = \sum_{\substack{\mathfrak{a}\subseteq A\\ \text{Ideal}\neq 0}} \frac{1}{N(\mathfrak{a})^s}$ für $\operatorname{Re} s > 1$.
(3) $\zeta_{\mathbb{Q}}(s) = \sum_{n\geq 1} \frac{1}{n^s} = \zeta(s)$.
(4) Sei $h = \#\mathcal{C}(K)$ die Klassenzahl von K, κ der Koeffizient von Satz 14.3, d.h. $i(\lambda) = h\kappa\lambda + O(\lambda^{1-1/m})$. Schreiben $\zeta_K(s) = \underbrace{\sum_{n\geq 1} \frac{j_n - h\kappa}{n^s}}_{=:f(s)} + h\kappa\zeta(s)$, für $\operatorname{Re}(s) > 1$.

Wegen $\sum_{n\leq\lambda} (j_n - h\kappa) = \kappa h\lambda + O(\lambda^{1-1/m}) - h\kappa\lfloor\lambda\rfloor = O(\lambda^{1-1/m})$ konvergiert $f(s)$ für $\operatorname{Re}(s) > 1-\frac{1}{m}$. Es folgt:

15.4 **Satz:** Es ist $h_K = \lim\limits_{\substack{s \downarrow 1 \\ (s \text{ reell})}} \frac{\zeta_K(s)}{\zeta(s)} = \lim\limits_{\substack{s \downarrow 1 \\ (s \text{ reell})}} (s-1)\zeta_K(s)$.

⌈Denn: $\zeta(s) = \frac{1}{s-1} \cdot g(s)$ mit $g(1) = 1$.⌋

15.5 **Bem.:** • Jedes Ideal $\mathfrak{a}$ ist eindeutig Produkt von Primidealen $\mathfrak{p} \neq 0$ von A, d.h. $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Somit ist $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$.
Dies ergibt (laut Eulerproduktsatz Anz 8.15(ii)) die folgende Darstellung von ζ_K als Eulerprodukt: $\zeta_K(s) = \sum\limits_{\substack{\mathfrak{a} \neq 0 \\ \text{Ideal}}} \frac{1}{N(\mathfrak{a})^s} = \prod\limits_{\mathfrak{p} \in \mathcal{P}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}$ für $\operatorname{Re} s > 1$,
wo $\mathcal{P} := \{\mathfrak{p} \subseteq A;\ \mathfrak{p} \text{ Ideal}, \mathfrak{p} \text{ prim}\}$.
• Behandeln Fall $n = 2$ jetzt genauer.

15.6 **Vor.:** Sei $K = \mathbb{Q}(\sqrt{d})$, wo $d \in \mathbb{Z}$, $\mu^2(d) = 1$, $d \neq 1$, dann ist $D := \operatorname{dis}(K) = \begin{cases} d, & d \equiv 1\ (4), \\ 4d, & d \equiv 2,3\ (4). \end{cases}$

15.7 **Lemma:** Es gibt einen (Dirichletschen) Zahlcharakter χ mod D, der sogenannte Charakter von K, mit: $\forall p \in \mathbb{P}$ gilt:
$$A_p = \begin{cases} \mathfrak{p}^2 \Leftrightarrow \chi(p) = 0, \\ \mathfrak{p}_1 \cdot \mathfrak{p}_2\ (\mathfrak{p} \neq \mathfrak{p}') \Leftrightarrow \chi(p) = 1, \\ \text{prim} \Leftrightarrow \chi(p) = -1. \end{cases}$$

Beweisskizze: • Sei $p > 2$. Dann: $A_p = \begin{cases} \mathfrak{p}^2 \Leftrightarrow p \mid d, \\ \mathfrak{p}_1 \cdot \mathfrak{p}_2 \Leftrightarrow p \nmid d \wedge \left(\frac{d}{p}\right) = 1, \\ \text{prim} \Leftrightarrow p \nmid d \wedge \left(\frac{d}{p}\right) = -1. \end{cases}$
(vgl. Z13.2 aus ZT I)
Mit dem QRG folgt, dass der Zerlegungstyp von A_p nur von der Restklasse von p mod $|D|$ abhängt. Genauer: Sei $\chi : \mathbb{Z} \to \mathbb{Z}$ definiert durch
(i) $(a, D) \neq 1 : \chi(a) := 0$, (ii) $(a, D) = 1 : \chi(a) := \begin{cases} \left(\frac{a}{|d|}\right), & \text{falls } d \equiv 1\ (4), \\ (-1)^{(a-1)/2} \left(\frac{a}{|d|}\right), & \text{falls } d \equiv 3\ (4), \\ (-1)^{(a^2-1)/8 + \frac{a-1}{2} \cdot \frac{d'-1}{2}} \left(\frac{a}{|d|}\right), & \text{falls } d \equiv 2\ (4), \end{cases}$ $2d' = d$.

χ ist dann ein Charakter mod D. Denn betr. etwa den Fall $d \equiv 1\ (4)$, $p > 2$, dann ist $D = d$ und $A_p = \begin{cases} \mathfrak{p}^2 \Leftrightarrow p \mid d \Leftrightarrow \chi(p) = 0, \\ \mathfrak{p}_1 \cdot \mathfrak{p}_2 \Leftrightarrow \left(\frac{d}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{|d|}\right) \overset{!}{=} \left(\frac{p}{d}\right) = 1, \\ \text{prim} \Leftrightarrow \left(\frac{d}{p}\right) = -1 \Leftrightarrow \left(\frac{p}{|d|}\right) = -1. \end{cases}$ ⌈"!": $d = -|d| \Rightarrow \left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{|d|}{p}\right)$⌋

• Ist $p = 2$, so gilt
$A \cdot 2 = \mathfrak{p}_2 \mathfrak{p}_2' \Leftrightarrow |d| \equiv 1\ (8) \Leftrightarrow d \equiv 1, 7\ (8) \Leftrightarrow \left(\frac{2}{d}\right) = 1$ nach dem 2. EG. □

15.8. Folgerung (ζ_K für quadratische ZK): Es ist nach 15.5 also

$$\zeta_K(s) = \prod_{p\in\mathbb{P}} \prod_{\mathfrak{p}|p} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}, \text{ also}$$

$$\prod_{\mathfrak{p}|p} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} = \begin{cases} \left(\frac{1}{1-1/p^s}\right)^2, & \chi(p)=1, \\ \frac{1}{1-1/p^{2s}}, & \chi(p)=-1, \\ \frac{1}{1-1/p^s}, & \chi(p)=0, \end{cases} \quad \text{für } \mathrm{Re}(s)>1.$$

Es folgt für $\mathrm{Re}(s)>1$:

$$\zeta_K(s) = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} \cdot \frac{1}{1-\frac{\chi(p)}{p^s}} = \zeta(s)\cdot \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi(p)}{p^s}}.$$

Somit:

$$\zeta_K(s) = \zeta(s)\cdot L(s,\chi).$$

15.9. Kor.: Es ist $h_K = L(1,\chi)$. ⌜Denn $h_K = \lim_{s\searrow 1} \frac{\zeta_K(s)}{\zeta(s)}$ nach 15.4.⌟

Zusammen mit Gaußsummen-Betrachtungen zu $L(1,\chi)$, s. a12/13, führt dies zur Klassenzahlformel für quadratische ZK in a16.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a16: Klassenzahlformel für quadratische ZK

Stichworte: Charakter χ eines quadr. ZKs K, Klassenzahlformel für h im reell- und imaginärquadratischen Fall, Reste und Nichtreste bzgl. χ

16.1. Einleitung: Wir leiten eine geschlossene Formel für die Klassenzahl h eines quadratischen ZKs K her. Es ergeben sich Erkenntnisse zu Resten und Nichtresten bezüglich des Charakters von K. Für reellquadratisches K spielt dabei die Grundeinheit eine wesentliche Rolle in der Klassenzahlformel.

16.2. Voraussetzung: $K = \mathbb{Q}(\sqrt{d})$ quadratischer ZK mit $d \neq 1$ quadratfrei und $q := |\mathrm{disc}(K)|$, sowie χ der Charakter von K (laut 15.7).

16.3. Satz: (i) χ ist ein primitiver Charakter mod q.
(ii) $d > 0 \Rightarrow \chi$ gerade, $d < 0 \Rightarrow \chi$ ungerade.

Bew.: (i): Es genügt z.z.: Zu jedem Primteiler p (>0) von q gibt es ein $a \in \mathbb{Z}$ mit $a \equiv 1 \pmod{\frac{q}{p}}$ und $\chi(a) = -1$.

$\ulcorner$ $a \in G_q \xrightarrow{s'} G_{q/p} \longrightarrow G_d$ und $d \mid q$,

$$\begin{tikzcd} G_q \arrow[r, two heads, "s'"] \arrow[dr, "\chi"'] & G_{q/p} \arrow[r] \arrow[d, dashed, "\chi'"] & G_d \arrow[dl, dashed] \\ & \mathbb{C}^\times & \end{tikzcd}$$

$s'(a) = 1$, $\underbrace{\chi(a)}_{= \chi'(s'(a)) = \chi'(1) = 1} = -1$. $\lightning$ $\lrcorner$

• Falls p ungerade: Für $a, b \in \mathbb{Z}$, $b > 0$ mit $(a, pb) = 1$ gilt nach Def. des Jacobi-Symbols: $\left(\frac{a}{pb}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. Sei nun $n \in \mathbb{Z}$ ein quadratischer Nichtrest mod p. Nach dem CRS ex. dann ein $a \in \mathbb{Z}$ mit

$$a \equiv 1 \begin{cases} \left(\frac{d}{p}\right), & \text{falls } 2 \nmid d, \\ \left(\frac{d'}{p}\right), & \text{falls } d = 2d' \text{ gerade } [d' \text{ ungerade, da } d \text{ quadratfrei}] \end{cases}$$

und $a \equiv 1 \ (8)$ und $a \equiv n \ (p)$.

Dann gilt nach Def von χ in 15.7:

→ Falls $d \equiv 1\ (4)$: $\chi(a) = \left(\frac{a}{|d|}\right) = \underbrace{\left(\frac{a}{p}\right)}_{-1} \cdot \underbrace{\left(\frac{a}{|d|/p}\right)}_{1} = -1.$

→ Falls $d \equiv 3\ (4)$: $\chi(a) = \underbrace{(-1)^{\frac{a-1}{2}}}_{=1} \left(\frac{a}{|d|}\right) = \underbrace{\left(\frac{a}{p}\right)}_{-1} \cdot \underbrace{\left(\frac{a}{|d|/p}\right)}_{1} = -1.$

· Falls $p=2$: Wegen $2 \mid m$ ist $d \equiv 2, 3\ (4)$.

→ Falls $d \equiv 3\ (4)$: Wählen $a \in \mathbb{Z}$ mit $a \equiv \begin{cases} 3\ (4), \\ 1\ (d). \end{cases}$

Dann ist $a \equiv 1\ (|2d|) = 1\left(\frac{q}{2}\right)$ und $\chi(a) = \underbrace{(-1)^{\frac{a-1}{2}}}_{-1} \cdot \underbrace{\left(\frac{a}{|d|}\right)}_{1} = -1.$

→ Falls $d = 2d'$: Wählen $a \in \mathbb{Z}$ mit $a \equiv \begin{cases} 5\ (8), \\ 1\ (d'). \end{cases}$

Dann ist $a \equiv 1\ (|4d'|) = 1\left(\frac{q}{2}\right)$ und $\chi(a) = \underbrace{(-1)^{\frac{a^2-1}{8} + \frac{a-1}{2} \cdot \frac{d'-1}{2}}}_{-1} \underbrace{\left(\frac{a}{|d'|}\right)}_{1} = -1.$

(::): → Falls $d \equiv 1\ (4)$: $\chi(-1) = \left(\frac{-1}{|d|}\right) \underset{\text{Euler}}{=} (-1)^{\frac{|d|-1}{2}} = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$

→ Falls $d \equiv 3\ (4)$: $\chi(-1) = -\left(\frac{-1}{|d|}\right) = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$

→ Falls $d = 2d'$: $\chi(-1) = (-1)^{\frac{d'-1}{2}} \left(\frac{-1}{|d'|}\right) = (-1)^{\frac{d'-1}{2} + \frac{|d'|-1}{2}} = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$ □

Erinnerung an die

16.4. Def.: Ein Gruppencharakter χ heißt quadratisch, falls $\chi^2 = 1$, d.h. falls $\operatorname{im} \chi \subseteq \{\pm 1\}$. (Auch: reell, Gegenteil: imaginär)

16.5. Bem.: Der Charakter eines quadratischen Zahlkörpers ist quadratisch.
⌜Jetzt klar: Werte $\in \{0, \pm 1\}$⌟

Wir können nun eine geschlossene Formel für die Klassenzahl h eines quadratischen Zahlkörpers beweisen.

16.6. Satz (Klassenzahlformel):

Sei $K = \mathbb{Q}(\sqrt{d})$, $0,1 \neq d \in \mathbb{Z}$ quadratfrei, $q := |\mathrm{disc}(K)|$, χ der Charakter von K und h die Klassenzahl von K. Dann gilt:

(i) Im reellquadratischen Fall (d.h. $d>0$):

$$h = -\frac{1}{\log(u)} \sum_{\substack{0<k<\frac{q}{2} \\ (k,q)=1}} \chi(k) \log\sin\left(\frac{k\pi}{q}\right),$$

wobei u die Grundeinheit >1 von K ist,

(ii) im imaginärquadratischen Fall (d.h. $d<0$) für $d \neq -1,-3$:

$$h = -\frac{1}{q} \sum_{\substack{0<k<q \\ (k,q)=1}} \chi(k)\, k \overset{\circledast}{=} \frac{1}{2-\chi(2)} \sum_{\substack{0<k<\frac{q}{2} \\ (k,q)=1}} \chi(k).$$

Bew.: Nach 15.9 ist $h\kappa = L(1,\chi)$.

Nun ist χ primitiv nach 16.3(i), also gilt nach 12.9:

$$L(1,\chi) = \begin{cases} -\dfrac{\tau_1(\chi)}{q} \displaystyle\sum_{\substack{0<k<q \\ (k,q)=1}} \bar{\chi}(k) \log\sin\left(\frac{k\pi}{q}\right), & \text{falls } d>0, \text{ d.h. } \chi \text{ gerade}, \\[2ex] \dfrac{\tau_1(\chi)\pi i}{q^2} \displaystyle\sum_{\substack{0<k<q \\ (k,q)=1}} \bar{\chi}(k)\, k, & \text{falls } d<0, \text{ d.h. } \chi \text{ ungerade}. \end{cases}$$

Nach 14.3 gilt:

$$\kappa = \begin{cases} \dfrac{2\log(u)}{\sqrt{q}}, & \text{falls } d>0, \\[2ex] \dfrac{\pi}{\sqrt{q}}, & \text{falls } d<-4, \text{ vgl. 26.13, (ZT I)} \rightsquigarrow \#A^\times = 2 \text{ oder } d=-2. \end{cases}$$

Da χ quadratisch, vgl. 16.5, ist $\bar{\chi} = \chi$. Eingesetzt:

$$h = \frac{L(1,\chi)}{\kappa} = \begin{cases} -\dfrac{\tau_1(\chi)}{2\log(u)\sqrt{q}} \displaystyle\sum_{\substack{0<k<q \\ (k,q)=1}} \chi(k) \log\sin\left(\frac{k\pi}{q}\right), & d>0, \\[2ex] \dfrac{\tau_1(\chi)}{q^{3/2}}\, i \displaystyle\sum_{\substack{0<k<q \\ (k,q)=1}} \chi(k)\, k, & d<-4 \text{ oder } d=-2. \end{cases}$$

• Für gerade χ gilt ($d>0$): $\displaystyle\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)\log\sin\left(\frac{k\pi}{q}\right)$

$$= \sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k)\log\sin\left(\frac{k\pi}{q}\right) + \sum_{\substack{0<k<q/2\\(k,q)=1}} \underbrace{\chi(q-k)}_{=\chi(-k)=\chi(k)} \underbrace{\log\sin\left(\frac{(q-k)\pi}{q}\right)}_{=\sin\left(\frac{k\pi}{q}\right)}$$

$$= 2\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k)\log\sin\left(\frac{k\pi}{q}\right),$$ d.h. mit 13.5 ($\tau_1(\chi)=\sqrt{q}$) ist

(i): $$h = -\frac{1}{\log(\alpha)}\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k)\log\sin\left(\frac{k\pi}{q}\right).$$

• Für ungerade χ gilt ($d<-4$ oder $d=-2$) mit 13.5 ($\tau_1(\chi)=i\sqrt{q}$) dann

(ii): $$h = -\frac{1}{q}\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k.$$

Zusatzformel (*):

• q gerade: Es ist $$\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k = \sum_{\substack{0<k<\frac{q}{2}\\(k,q)=1}} \chi(k)k + \sum_{\substack{0<k<\frac{q}{2}\\(k,q)=1}} \overbrace{\chi(k+\tfrac{q}{2})}^{\overset{(0)}{=}\chi(-k)=-\chi(k)}\cdot(k+\tfrac{q}{2})$$

$$= -\frac{q}{2}\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k) \Rightarrow \frac{1}{2-\chi(2)}\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k) = h,$$ da $\chi(2)=0$ für $2\mid q$.

Zu (0): Für ungerade k ist $\chi(k+\frac{q}{2}) = -\chi(k)$.

⌜Da $4\mid q$, ist $(\frac{q}{2}+1)^2 = \underbrace{\frac{q}{4}}_{\in\mathbb{Z}}\cdot q + q + 1 \equiv 1\ (q)$.

Das von $\frac{q}{2}$ in $\mathbb{Z}/q$ erzeugte Ideal besteht aus $0, \frac{q}{2}$.

Da χ primitiv ist, gilt $\chi(1+\frac{q}{2}) = -1$,

denn sonst würde χ auf $\ker(G_q \to G_{q/2}) = \{1, 1+\frac{q}{2}\}$ trivial sein.

⌜Sonst:
$$\begin{tikzcd}
\mathbb{Z}/q \arrow[r, two heads] & \mathbb{Z}/\frac{q}{2} \\
(\mathbb{Z}/q)^* \arrow[u, phantom, "\cup\!\mid"] \arrow[r, two heads, "\varphi"] \arrow[dr, "\chi"'] & (\mathbb{Z}/\frac{q}{2})^* \arrow[u, phantom, "\cup\!\mid"] \arrow[d, dashed, "\chi'"] \\
 & \mathbb{C}^1
\end{tikzcd}$$

$\ker(\varphi) = \{1+\frac{q}{2}, 1\} \subseteq \ker(\chi)$ ⌟

Nun ist für k ungerade $\frac{q}{2}k \equiv \frac{q}{2}\ (q)$ erfüllt,

also ist $(\frac{q}{2}+1)k \equiv \frac{q}{2}+k\ (q)$.

Es folgt: $\chi(\frac{q}{2}+k) = \chi((\frac{q}{2}+1)k) = \underbrace{\chi(\frac{q}{2}+1)}_{=-1}\chi(k) = -\chi(k)$. ⌟

• q ungerade: Es ist $\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k = \sum_{\substack{0<k<\frac{q}{2}\\(k,q)=1}} \chi(k)k + \sum_{\substack{0<k<q/2\\(k,q)=1}} \overbrace{\chi(q-k)}^{=\chi(-k)=-\chi(k)}\cdot(q-k)$

$$= 2\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k)k - q\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k). \qquad (\mathrm{I})$$

Andererseits ist $\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k = \sum_{\substack{0<k<\frac{q}{2}\\(k,q)=1\\k \text{ gerade}}} \chi(k)k + \sum_{\substack{0<k<\frac{q}{2}\\(k,q)=1\\k \text{ gerade}}} \chi(\underbrace{q-k}_{\text{ungerade}})\cdot(q-k)$

$$= \sum_{\substack{0<k<q/2\\(2k,q)=1}} \chi(2k)\cdot 2k + \sum_{\substack{0<k<q/2\\(2k,q)=1}} \underbrace{\chi(q-2k)}_{-\chi(2k)}\cdot(q-2k)$$

$$= 4\chi(2)\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k)k - q\chi(2)\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k). \qquad (\mathrm{II})$$

Die Berechnung $2\cdot(\mathrm{I})-(\mathrm{II})\cdot\chi(2)$ liefert nun, da $\chi^2=1$:

$$(2-\chi(2))\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k = -q\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k), \text{ also ist}$$

$$h = -\frac{1}{q}\sum_{\substack{0<k<q\\(k,q)=1}} \chi(k)k = \frac{1}{2-\chi(2)}\sum_{\substack{0<k<q/2\\(k,q)=1}} \chi(k).$$

$\square$

16.7. Folgerungen:

(1) Für $d>0$ seien $R := \{k\in(\mathbb{Z}/q)^*;\ 0<k<\frac{q}{2},\ \chi(k)=1\}$ die Reste, und $N := \{k\in(\mathbb{Z}/q)^*;\ 0<k<\frac{q}{2},\ \chi(k)=-1\}$ die Nichtreste.

Sei

$$v := \frac{\prod_{k\in N}\sin\left(\frac{k\pi}{q}\right)}{\prod_{k\in R}\sin\left(\frac{k\pi}{q}\right)}.$$

Dann gilt: $u^h = v$. Insbesondere ist $v>1$.

Sei $d=p>0$ prim, $p\equiv 1\,(4)$. Dann ist $\chi(k)=\left(\frac{k}{p}\right)$, und somit $\prod_{k\in N}\sin\left(\frac{k\pi}{p}\right) > \prod_{k\in R}\sin\left(\frac{k\pi}{p}\right)$.

(2) Sei $p>2$ prim, $p\equiv 3\,(4)$, und $d=-p$. Wegen $d\equiv 1\,(4)$ ist $\chi(a)=\left(\frac{a}{p}\right)$. Die Anzahl der Summanden von $\sum_{\substack{k\in(\mathbb{Z}/p)^*\\0<k<p/2}}\chi(k)$ ist $\frac{p-1}{2}$, also ungerade.

Weiter ist $\chi(2)=\left(\frac{2}{p}\right)=\begin{cases}-1, & p\equiv 3\,(8),\\ 1, & p\equiv 7\,(8).\end{cases}$

Mit R, N wie in (1) definiert folgt: $h = \begin{cases}\#R-\#N, & p\equiv 7\,(8),\\ \frac{1}{3}(\#R-\#N), & p\equiv 3\,(8).\end{cases}$

16.8. **Bsp.:** • Sei $p = 19 \equiv 3\ (8)$, $d = -19$.

Bestimme $\#R$ und $\#N$: Haben $\chi(a) = \left(\frac{a}{p}\right)$, und eine Tabelle aller quadratischen Reste mod 19:

k	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8	9
k^2	$\underline{\underline{1}}$	$\underline{\underline{4}}$	$\underline{\underline{9}}$	-3	$\underline{\underline{6}}$	-2	-8	$\underline{\underline{7}}$	$\underline{\underline{5}}$,

für $\#R$ werden nur die qu. Reste >0 und $< \frac{19}{2} = 9.5$ gezählt (unterstrichen), also $\#R = 6$. Für $\#N$ die Nichtreste in $\{2, \dots, 9\}$, das sind $2, 3, 8$, also $\#N = 3$. Wir erhalten laut 16.7(2): $h = \frac{1}{3}(\#R - \#N) = \frac{1}{3}(6-3) = \underline{\underline{1}}$.

Somit ist $\mathbb{Q}(\sqrt{-19})$ faktoriell.

• Betrachte $\mathbb{Q}(\sqrt{2})$ mit der GE $u = 1 + \sqrt{2}$, $\operatorname{disc}(\mathbb{Q}(\sqrt{2})) = 8$. Dann:

$$h = -\frac{1}{\log(1+\sqrt{2})}\left(\underbrace{\chi(1)}_{=1}\log\sin\frac{\pi}{8} + \underbrace{\chi(3)}_{=-1}\log\sin\frac{3\pi}{8}\right) = \frac{\log(\sin(3\pi/8)/\sin(\pi/8))}{\log(1+\sqrt{2})}$$

$$\overset{TR}{=} \frac{\log(0.9239/0.3827)}{\log(2.4142)} \approx \frac{0.8814}{0.8814} = 1, \quad \text{also } \underline{\underline{h = 1}}.$$

• Betrachte $\mathbb{Q}(\sqrt{13})$, haben $u = \frac{3}{2} + \frac{1}{2}\sqrt{13}$ laut Bsp. Z25.15 in ZT I.

$\rightsquigarrow \operatorname{disc}\mathbb{Q}(\sqrt{13}) = 13$

Dann ist laut Klassenzahlformel

$$h = -\frac{1}{\log(u)}\sum_{\substack{0<k<\frac{13}{2}\\(k,13)=1}} \chi(k)\log\sin\left(\frac{k\pi}{13}\right),$$

wo $\chi(k) = \left(\frac{k}{13}\right)$ ist wegen $13 \equiv 1\ (4)$.

Tabelle der quadr. Reste mod 13:

a	± 1	± 2	± 3	± 4	± 5	± 6
a^2	1	4	-4	3	-1	-3

Somit ist

$$h = -\frac{1}{\log\left(\frac{3}{2}+\frac{1}{2}\sqrt{13}\right)}\cdot\Big(\underbrace{\chi(1)}_{=1}\cdot\log\sin\left(\tfrac{\pi}{13}\right) + \underbrace{\chi(2)}_{=-1}\cdot\log\sin\left(\tfrac{2\pi}{13}\right) + \underbrace{\chi(3)}_{=1}\cdot\log\sin\left(\tfrac{3\pi}{13}\right)$$

$$+ \underbrace{\chi(4)}_{=1}\cdot\log\sin\left(\tfrac{4\pi}{13}\right) + \underbrace{\chi(5)}_{=-1}\cdot\log\sin\left(\tfrac{5\pi}{13}\right) + \underbrace{\chi(6)}_{=-1}\cdot\log\sin\left(\tfrac{6\pi}{13}\right)\Big)$$

$$\overset{TR}{=} -0.8370\cdot\big(1\cdot(-1.4300) + (-1)\cdot(-0.7663) + 1\cdot(-0.4108)$$
$$+ 1\cdot(-0.1948) + (-1)\cdot(-0.0672) + (-1)\cdot(-0.0073)\big)$$

$= 1.0000 \rightsquigarrow$ also $\underline{h = 1}$

• Betrachte $\mathbb{Q}(\sqrt{17})$, haben $u = 4+\sqrt{17}$, $\operatorname{disc}\mathbb{Q}(\sqrt{17}) = 17$

Dann ist laut Klassenzahlformel

$$h = -\frac{1}{\log(u)} \sum_{\substack{0<k<\frac{17}{2} \\ (k,17)=1}} \chi(k) \log\sin\left(\frac{k\pi}{17}\right),$$ wo $\chi(k) = \left(\frac{k}{17}\right)$ ist wegen $17 \equiv 1 (4)$

Tabelle der quadr. Reste mod 17

a	±1	±2	±3	±4	±5	±6	±7	±8
a^2	1	4	-8	-1	8	2	-2	-4

Somit ist

$$h = -\frac{1}{\log(4+\sqrt{17})} \cdot \Big(\underbrace{\chi(1)}_{=1} \cdot \log\sin\left(\tfrac{\pi}{17}\right) + \underbrace{\chi(2)}_{=1} \cdot \log\sin\left(\tfrac{2\pi}{17}\right) + \underbrace{\chi(3)}_{=-1} \cdot \log\sin\left(\tfrac{3\pi}{17}\right)$$

$$+ \underbrace{\chi(4)}_{=1} \cdot \log\sin\left(\tfrac{4\pi}{17}\right) + \underbrace{\chi(5)}_{=-1} \cdot \log\sin\left(\tfrac{5\pi}{17}\right) + \underbrace{\chi(6)}_{=-1} \cdot \log\sin\left(\tfrac{6\pi}{17}\right)$$

$$+ \underbrace{\chi(7)}_{=-1} \cdot \log\sin\left(\tfrac{7\pi}{17}\right) + \underbrace{\chi(8)}_{=1} \cdot \log\sin\left(\tfrac{8\pi}{17}\right) \Big)$$

$$\overset{TR}{=} -0.0478 \cdot \big(1 \cdot (-1.6942) + 1 \cdot (-1.0182) + (-1) \cdot (-0.6416)$$
$$+ 1 \cdot (-0.3950) + (-1) \cdot (-0.2256) + (-1) \cdot (-0.1107)$$
$$+ (-1) \cdot (-0.0389) + 1 \cdot (-0.0043) \big)$$

$$= \underline{\underline{1.0000}}$$ Also $h = 1$

• Betr. $\mathbb{Q}(\sqrt{5})$, $u = \frac{1}{2} + \frac{1}{2}\sqrt{5}$

da $\left(\frac{2}{5}\right) = -1$

$$h = -\frac{1}{\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)} \left(\log\sin\left(\tfrac{\pi}{5}\right) - \log\sin\left(\tfrac{2\pi}{5}\right) \right) = -2.0781(-0.5314 + 0.0502)$$

$$\overset{TR}{=} \underline{\underline{1.0000}}$$

• Betr. $\mathbb{Q}(\sqrt{-5})$, $-5 \equiv 3 (4) \rightsquigarrow \operatorname{disc}\mathbb{Q}(\sqrt{-5}) = -20$, $q = 20$.

Haben $\chi(a) = (-1)^{(a-1)/2} \left(\frac{a}{5}\right)$ laut 15.7, ist Charakter mod 20.

Weiter: $\chi(3) = (-1) \cdot \left(\frac{3}{5}\right) = 1$, $\chi(7) = (-1)^3 \cdot \left(\frac{7}{5}\right) = 1$, $\chi(2) = 0$,

also ist laut 16.6.(ii) dann $h = \frac{1}{2 - \underbrace{\chi(2)}_{=0}} \sum_{\substack{(k,q)=1 \\ 0<k<10}} \chi(k)$,

also

$$h = \frac{1}{2}\big(\overbrace{\chi(1)}^{=1} + \overbrace{\chi(3)}^{=1} + \overbrace{\chi(7)}^{=1} + \overbrace{\chi(9)}^{=1}\big) = \underline{\underline{2}}.$$ Der ZR ist nicht faktoriell.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a17: Siebmethoden

Stichworte: Konzept Sieb, Siebfunktion PZ Zwillingssieb, Polignac-Vermutung, Satz von Brun/Chen, Pentium-Bug, große und kleine Siebe, Quasiquadrate, kl. quNR

17.1. Einleitung: Wir führen das Konzept eines mathematischen Siebs ein.

Vorbild: Sieb des Eratosthenes: Sei $x>0$ und $\mathcal{A} := \{n \le x\}$, etwa $x = 25$: ($\sqrt{25}=5$)

(1) ~~2~~ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

Für jede PZ $p \le \sqrt{x}$ streiche alle $\lfloor \frac{x}{p} \rfloor$ Vielfachen von p, in der Liste verbleiben alle Primzahlen zwischen $\sqrt{x}$ und x (Funktioniert, da zusammengesetzte Zahlen $\le x$ einen Primteiler $\le \sqrt{x}$ besitzen).

17.2. Formalisierung eines Siebproblems: Sei $\mathcal{A}$ eine endliche Menge. Sei $\mathcal{P}$ die Menge der PZen p, für die es eine bestimmte Teilmenge $\mathcal{A}_p \subseteq \mathcal{A}$ gibt.
Problem: Bestimme gute o.S. und u.S. für die Kardinalität der gesiebten Menge $\mathcal{S}(\mathcal{A},\mathcal{P}) := \mathcal{A} \setminus \bigcup_{p\in\mathcal{P}} \mathcal{A}_p$, der Siebfunktion $\#\mathcal{S}(\mathcal{A},\mathcal{P})$.
Mathematisch praktikabel ist die folgende, moderne Notation für ein Siebproblem (eine endl. Folge $(a_n)_{n\le x}$ als $\mathcal{A}$ zu nehmen erlaubt Wiederholungen in der "Liste" der zu streichenden Objekte/Zahlen):

17.3. Def.: Sei $\mathcal{A}=(a_n)_{n\le x}$ eine endliche Folge (typischerweise nat. Zahlen), $\mathcal{P} \subseteq \mathbb{P}$. Für ein $z>1$ reell def. $P(z) := \prod_{\substack{p\in\mathcal{P}\\ p<z}} p$. Die Daten $(\mathcal{A},\mathcal{P},z)$ heißen Sieb.

17.4. Bsp.: Im Eratosthenes-Sieb: $\mathcal{P}=\mathbb{P}$, $a_n = n$, $z=\sqrt{x}$. Die Vielfachen a_n von $p<z$ werden "gestrichen", "mit 0 überschrieben", "fallen durch das Sieb". Im Sieb "übrig" bleiben alle ungestrichenen $a_n = n \le x$, das sind die $n \le x$, wo $ggT(n, P(z)) = 1$.

17.5. **Def.:** In einem Sieb heißt $S(\mathcal{A},\mathcal{P},z) := \sum_{\substack{n\le x\\ (a_n,P(z))=1}} 1$ die Siebfunktion.

17.6. **Bsp.:** Im Eratosthenes-Sieb ist $S(\mathcal{A},\mathcal{P},\sqrt{x})$ die Kardinalität der ungestrichenen Zahlen zwischen $\sqrt{x}$ und x, genau: $S(\mathcal{A},\mathcal{P},\sqrt{x}) = \pi(x) - \pi(\sqrt{x})$.
[Wähle $a_1=0$, sonst $a_n=n$ für $n>1$. Ist $\sqrt{x}\in\mathbb{Z}$, nimm $z=\sqrt{x}+\frac{1}{2}$.]

17.7. **Bsp.:** PZ Zwillingssieb: $a_n := n(n+2)$, $\mathcal{P}=\mathbb{P}$, $x>2$, $z\ge 2$.
Sei $S(\mathcal{A},\mathcal{P},z) = \#\{n\le x;\ (a_n, P(z))=1\}$ die Siebfunktion.
Ist $z>\sqrt{x}+2$, zählen wir mit der Siebfunktion alle PZen p, für die auch $p+2$ PZ ist, d.h. die gesiebte Menge besteht zwischen $\sqrt{x}$ und x genau aus den Primzahlzwillingen $p\in\mathbb{P}$, für die auch $p+2\in\mathbb{P}$ ist.

17.8. PZ Zwillingsvermutung: Es gibt unendl. viele PZ Zwillinge.
Diese Vermutung ist bis heute unbewiesen! Die Siebtheorie kennt Teilantworten, die wir in diesem Kapitel besprechen möchten. Eine Verfeinerung von 17.8 lautet:

17.9. PZ Zwillingsvermutung nach Hardy-Littlewood: Sei $\pi_2(x) := \#\{p\le x;\ p,p+2\in\mathbb{P}\}$.
Dann gilt $\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{\log^2(t)} \sim 2C_2 \frac{x}{\log^2(x)}$ mit $C_2 := \prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = 0.66016\ldots$
Die Konstante $C_2>0$ heißt Zwillingskonstante.

Zur Abschätzung von Siebfunktionen kennt man Siebsätze.
Dazu gehören klassischerweise das Brunsche Sieb und das Selberg-Sieb.
Da das große Sieb eines der neueren ist und stärker als die genannten, wollen wir dieses hier besprechen und zeigen, dass damit die meisten gängigen Anwendungen zu bewerkstelligen sind.
So zeigen wir in a20.10 das folgende Ergebnis (nur für $n=2$, allg. $n\in\mathbb{N}_{\ge 2}$ analog).

17.10. **Satz:** Sei $\pi_n(x) := \#\{p\in\mathbb{P};\ p\le x,\ p+n\in\mathbb{P}\}$ für $2\mid n$,
insb. ist $\pi_2(x)$ die Anzahl der PZ Zwillinge $\le x$.
Dann ist $\pi_n(x) \ll \frac{x}{\log^2(x)} \prod_{p\mid n}\left(1+\frac{1}{p}\right)$ mit absoluter impliziter Konstante. [Nathanson, Thm. 7.2]

17.11. **Bem.:** Die Vermutung von de Polignac (1849) besagt $\pi_n(x) \xrightarrow{x\to\infty} \infty$ für alle geraden $n \in \mathbb{N}$.

Für den Fall $n=2$ hatten wir fest (und gilt nach a20.10):

17.12. **Kor.:** Es ist $\pi_2(x) \ll \frac{x}{\log^2(x)}$.

17.13. **Kor./Satz von Brun:** Sei p_n die (aufsteigende) Folge der PZ Zwillinge p_n (mit $p_n+2 \in \mathbb{P}$).
Dann ist $\sum_{n\geq 1} \left(\frac{1}{p_n} + \frac{1}{p_n+2}\right)$ konvergent. (Bew. $\sum_{n\geq 1} \frac{1}{p_n}$ kgt.)

Bew.: $n = \pi_2(p_n) \ll \frac{p_n}{\log^2(p_n)}$, also ist $\frac{1}{p_n} \ll \frac{1}{n \log^2(p_n)} \ll \frac{1}{n \log^2(n)}$,
und daher

$$\sum_{n\geq 1} \frac{1}{p_n} \ll \sum_{n\geq 1} \frac{1}{n \log^2(n)}, \text{ was kgt.} \qquad \square$$

Brun zeigte diesen Satz 1920 mit einem anderen Siebsatz, der Brunsches Sieb heißt.

17.14. **Bem.:** Der Satz von Brun besagt, dass es deutlich weniger PZ Zwillinge gibt als Pzen. Die offene Frage, ob $\pi_2(x)$ divergiert, d.h. 17.8, bleibt damit aber ungeklärt.

17.15. **Def.:** Die Konstante $\sum_{\substack{p,\, p+2 \\ \text{prim}}} \left(\frac{1}{p} + \frac{1}{p+2}\right) = 1{,}9021604 \pm 5 \cdot 10^{-7}$ heißt auch Brunsche Konstante.

17.16. Beim Versuch, diesen numerischen Wert genauer zu bestimmen, fand T. Nicely im Jahr 1995 einen Bug (= Programmierfehler) im damaligen Intel Pentium Computer Chip. Die Behebung dieses Fehlers hat die Firma Intel viele Millionen Dollar gekostet.

Als bisher bestes Resultat in Richtung PZ Zwillingsvermutung wird folgendes Resultat von 1973 angesehen:

17.17. **Satz von Chen:** Es gibt unendl. viele $p \in \mathbb{P}$, so dass $\Omega(p+2) \leq 2$ gilt, wobei $\Omega(n) := \sum_{p^\alpha \mid n} 1$ die Anzahl der Primfaktoren von n bezeichnet.

Der Beweis dieses Satzes erfordert stark verfeinerte, umfangreiche Siebmethoden. Er kann z.B. nachgelesen werden in [Nathanson, Additive Number Theory – The Classical Bases, Chap. 9 & 10].

Wir kommen nun zum großen Sieb:

17.18 Motivation: • Im PZzwillingssieb werden pro PZ $p>2$ die Streichungsreste 0 und -2 mod p benutzt. (Streichen a_n, bzw. setze $a_n=0$, falls $n\equiv 0(p)$ oder $n\equiv -2(p)$ ist).
• Im Sieb des Eratosthenes wird der Streichungsrest 0 mod p benutzt.

17.19. Def.: Für eine Zahlenfolge $\mathcal{A}=(a_n)_{n\in\mathbb{N}}$, $p\in\mathcal{P}\subseteq\mathbb{P}$ ist $W_p:=\{h\ (p);\ n\equiv h(p)\Rightarrow a_n=0\}$ die Menge der Streichungsrestklassen mod p, und $w(p):=\#W_p\leq p$ ihre Anzahl.
Es Siebprobleme, die wesentlich mehr Streichungsreste verwenden:
Bsp. Quasiquadrate:

17.20. Def.: $n\in\mathbb{N}$ heißt Quasiquadrat, falls $n\equiv x^2\ (p)$ für jedes $p\leq n^{1/2}$ lösbar ist, d.h. falls n für jedes $p\leq n^{1/2}$ ein quadratischer Rest mod p ist.
Quadratzahlen sind Quasiquadrate, aber umgekehrt muss dies nicht so sein.
Man gelangt zu der Frage, wieviele Quasiquadrate im Vergleich zu Quadratzahlen es gibt. Man kann diese mit einem Sieb zählen:

17.21. Sei $\mathcal{A}=(a_n)_{n\leq x}$ eine Folge in $\mathbb{Z}$, $\mathcal{P}=\mathbb{P}$. Sei $w(p)$ die Anzahl der Streichungsrestklassen mod p. Wir nehmen an, dass $w(p)<p$ für alle $p\in\mathcal{P}$ sei.
Für Quasiquadrate: $a_n:=\begin{cases}1, & n \text{ Quasiquadrat in } [\frac{x}{2},x],\\ 0, & \text{sonst für } n\leq x.\end{cases}$
Sei $p\leq\sqrt{\frac{x}{2}}=:z$.
Für ein Quasiquadrat ist $n\equiv h\ (p)$ nicht möglich für einen Rest h mod p, wenn $\nexists\, k: h\equiv k^2\ (p)$ gilt, d.h. wenn h kein quadratischer Rest mod p.
Solche Reste sind Streichungsreste. Die Anzahl der Quasiquadrate in $[\frac{x}{2},x]$ ist dann $\sum_{n\leq x} a_n$.
Für jede PZ $p\in\mathbb{P}$ gibt es $\frac{p-1}{2}$ quadratische Reste und ebensoviele Restklassen, die es nicht sind (die quadratischen Nichtreste).
⌈Ist $H=\{1,2,\dots,\frac{p-1}{2}\}$, so hat für einen qu. Rest a mod p die (lösbare) Kongruenz $x^2\equiv a\ (p)$ genau eine Lsg. in H: $b^2\equiv a\equiv c^2\ (p)\overset{\mathbb{Z}/p \text{ Körper}}{\Longrightarrow} b\equiv\pm c\ (p)$, also $b=c$, falls $b,c\in H$.⌋
Die # der qu. Reste ist also $\#H=\frac{p-1}{2}$, die der Nichtreste $=p-1-\frac{p-1}{2}=\frac{p-1}{2}$ ✓
Somit: Die $\frac{p-1}{2}$ vielen quadratischen Nichtreste sind Streichungsrestklassen mod p, haben so $w(p)\geq\frac{p-1}{2}$ im Sieb für Quasiquadrate.

17.22. **Bezeichnung:** Ein Sieb mit $\frac{w(p)}{p} > c$ für ein $c > 0$ und alle $p \in \mathcal{P}$ heißt großes Sieb (anschaulich: mit "großen" Löchern, durch die Zahlen fallen können). Andernfalls heißt das Sieb kleines Sieb.

17.23. **Bem:** Das genannte Sieb für Quasiquadrate ist ein großes Sieb, das für PZZwillinge und das Sieb des Eratosthenes sind Beispiele für kleine Siebe. Speziell für große Siebe ist der folgende Siebsatz gut geeignet. Er geht auf Linnik (1941) zurück und wurde von Bombieri, Montgomery, Vaughan u.a. weiterentwickelt.

17.24. **Satz vom großen Sieb:** Sei $\mathcal{A} = (a_n)_{n \le N}$ eine Folge in $\mathbb{C}$, $w(p)$ wie in Def. 17.19 und sei $w(p) < p$ für alle $p \in \mathcal{P}$. Setze $g_w(q) := \mu^2(q) \prod_{\substack{p \mid q \\ p \in \mathcal{P}}} \frac{w(p)}{p - w(p)}$ und $L_w := \sum_{q \le Q} g_w(q)$ für $Q \ge 1$ beliebig. Dann ist

$$\Big|\sum_{n \le N} a_n\Big|^2 \le \frac{N + Q^2}{L_w} \sum_{n \le N} |a_n|^2.$$

- Ist $\mathcal{A}$ speziell die charakteristische Fkt. einer Menge $\mathcal{M} \subseteq \mathbb{N} \cap [1, N]$ (gesiebt mit $w(p)$ vielen Restklassen mod p für alle $p \le Q$), d.h. $a_n = \begin{cases} 1, & n \in \mathcal{M}, \\ 0, & n \notin \mathcal{M}, \end{cases}$ dann folgt $\underbrace{\sum_{n \le N} a_n}_{= S(\mathcal{A}, \mathcal{P}, Q)} = \# \mathcal{M} \le \frac{N + Q^2}{L_w}$.

17.25. **Bem.:** Die Schranke hängt nur von $w(p)$ ab, nicht von der Art der benutzten Streichungsrestklassen. Ist $w(p) > cp$, ist $\frac{w(p)}{p - w(p)} = \frac{1}{p/w(p) - 1}$ groß und $\frac{1}{L_w}$ klein, die Schranke in 17.24 also gut. Der Satz gibt aber selbst für kleine Siebe meist außerordentlich gute Schranken.

Weiter ist Q nichts anderes als $Q = z$, die maximale Größe der Streichungsprimzahlen.

17.26. **Kor. / Satz über Quasiquadrate:** Ist $\mathcal{Q} = \{n \le x;\ n \text{ Quasiquadrat}\}$, so gilt $\# \mathcal{Q} \ll x^{1/2} \log(x)$ für $x \to \infty$. Die Größenordnung für die Anz Quasiquadrate ist in etwa vergleichbar mit der Anz. Quadratzahlen $\le x$. $\left[\frac{\# \mathcal{Q}}{x^{1/2}} \ll \log(x)\right]$

Bew.: Der Satz 17.24 vom großen Sieb mit $w(p) \geq \frac{p-1}{2}$, $N = x$ und a_n wie in 17.21 ergibt für die Anzahl $Q_1(x) := \sum_{\frac{x}{2} < n \leq x} a_n$ der Quasiquadrate in $[\frac{x}{2}, x]$ dann
$Q_1(x) \leq \frac{x + Q^2}{L_w}$, mit $Q := \sqrt{\frac{x}{2}}$ gibt dies $\ll \frac{x}{L_w}$.
Nun gilt für $q = p \leq Q$, dass $\frac{w(p)}{p - w(p)} \geq \frac{\frac{p-1}{2}}{p - \frac{p-1}{2}} = \frac{p-1}{p+1} \geq \frac{1}{3}$,
also $L_w \gg \sum_{p \leq Q} \frac{1}{3} \gg_{\text{Tsch.}} \frac{Q}{\log(Q)}$ und $Q_1(x) \leq \frac{x}{Q} \log(Q) \ll \sqrt{x} \log(x)$.
Für die Anzahl $\# \mathcal{Q}$ ergibt sich
$$\# \mathcal{Q} \ll \sum_{0 \leq k \leq \frac{\log(x)}{\log(2)}} Q_1\left(\frac{x}{2^k}\right) \ll \sqrt{x} \log(x) \sum_k \frac{1}{2^{k/2}} \ll \sqrt{x} \log(x).$$
□

Eine weitere Anwendung des großen Siebes 17.24 ist, damit mit quadratischen Resten zu sieben, um die Größe des kleinsten quadratischen Nichtrests mod $p \leq x$ zu bestimmen.

17.27. Def.: $n_p := \min\{n \in \mathbb{N};\ n \equiv X^2 (p) \text{ unlösbar in } X \bmod p\}$ heißt kleinster quadratischer Nichtrest.

Über die Größe von n_p gibt es folgende Vermutung:

17.28. Vermutung (von Vinogradov): $n_p \ll p^\varepsilon$ für alle $\varepsilon > 0$.
Bisher bekannt: Dies gilt für alle $\varepsilon > \frac{1}{4\sqrt{e}} = 0.1516\ldots$

17.29. Satz von Ankeny: GRH (für alle $L(s,\chi)$ mit $\chi \bmod p$) $\Rightarrow n_p \ll \log^2(p)$.
Für die algorithmische ZT spielt dies eine große Rolle. [Bew. in Vorl. Kryptographie]
[Polya-Vinogradov $\rightsquigarrow n_p \ll \sqrt{p} \log(p)$ laut Ü]

In diesem Zusammenhang zeigte Linnik (wofür er das große Sieb entwickelte):

17.30. Satz von Linnik: Die Anzahl der $p \leq x$ mit $n_p > x^\varepsilon$ ist beschränkt durch eine Konstante $C_\varepsilon > 0$. (D.h. Ausnahmen zur Vermutung 17.28 sind selten.)

Bew.: Betr. das Sieb $\mathcal{A} = (a_n)_{n \leq x}$ mit $a_n = n$, als Streichungs-P-menge nehmen wir diesmal $\mathcal{P} := \{p \in \mathbb{P};\ n \equiv X^2 (p) \text{ lösbar für alle } n \leq x^\varepsilon\}$,
und Streichungsrestklassen sind die $h \bmod p$, für die $h \equiv X^2 (p)$ unlösbar ist (d.h. qu. Nichtrest), haben also $w(p) \geq \frac{p-1}{2}$. Die gesiebte Menge ist $\mathcal{S}(\mathcal{A}, \mathcal{P}, \sqrt{x}) = \{n \leq x;\ n \equiv X^2 (p) \text{ lösbar für alle } p \in \mathcal{P}, p \leq \sqrt{x}\}$,
sei $S(\mathcal{A}, \mathcal{P}, \sqrt{x}) := \# \mathcal{S}(\mathcal{A}, \mathcal{P}, \sqrt{x})$.

Die Menge $\mathcal{S}(\mathcal{A},\mathcal{P},\sqrt{x})$ enthält insb. alle $m \le x$, die frei von Primteilern $> x^{\varepsilon}$ sind.
⌈Ist $m = p_1 \cdots p_r$, die $p_i \le x^{\varepsilon}$, so ist jede Kongruenz $p_i \equiv X^2 (p)$ lösbar, da $p_i \le x^{\varepsilon}$ und $p \in \mathcal{P}$, etwa mit X_i mod $p \rightsquigarrow X := X_1 \cdots X_r$ löst $m = p_1 \cdots p_r \equiv X^2 (p)$. Also: $m \in \mathcal{S}(\mathcal{A},\mathcal{P},\sqrt{x})$.⌋
Insb.: alle $m = n\, p_1 \cdots p_k \le x$ mit $x^{\varepsilon - \varepsilon^2} < p_j < x^{\varepsilon}$ für $1 \le j \le k = \lfloor \frac{1}{\varepsilon} \rfloor$, ein $n \in \mathbb{N}$.
(Beachte $n \le \frac{x}{p_1 \cdots p_k} \ll \frac{x}{x^{(\varepsilon-\varepsilon^2)/\varepsilon}} = \frac{x}{x^{1-\varepsilon}} = x^{\varepsilon}$, d.h. $p \mid m \Rightarrow p < x^{\varepsilon}$.)

Es folgt $S(\mathcal{A},\mathcal{P},\sqrt{x}) \ge \sum_{p_1 \cdots p_k} \left\lfloor \frac{x}{p_1 \cdots p_k} \right\rfloor \gg x \sum_{p \in [x^{\varepsilon-\varepsilon^2}, x^{\varepsilon}]} \frac{1}{p} \underset{\text{Mertens}}{\gg} x \underbrace{(\log\log x^{\varepsilon} - \log\log x^{\varepsilon-\varepsilon^2})}_{= \log \varepsilon - \log(\varepsilon - \varepsilon^2) = \log \frac{1}{1-\varepsilon} = C_{\varepsilon} > 0} \gg x.$

Das große Sieb zeigt andererseits, dass $S(\mathcal{A},\mathcal{P},\sqrt{x}) \ll \frac{x}{\sum_{\substack{p \in \mathcal{P} \\ p < \sqrt{x}}} 1}$,
denn $\frac{\omega(p)}{p - \omega(p)} = \frac{\frac{p-1}{2}}{p - \frac{p-1}{2}} = \frac{p-1}{p+1} \ge \frac{1}{3}$,

insg. folgt $\sum_{\substack{p \in \mathcal{P} \\ < \sqrt{x}}} 1 \ll \frac{x}{S(\mathcal{A},\mathcal{P},\sqrt{x})} \ll 1$, also $\#\mathcal{P} \ll_{\varepsilon} 1$. $\square$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a18: Das große Sieb

Stichworte: Das große Sieb (nach Montgomery), große-Sieb-Ungleichung

18.1. Einleitung: Wir zeigen den Satz vom großen Sieb, manchmal Montgomerys Sieb genannt. Alle Siebanwendungen dieser Vorlesung benutzen dieses Sieb, bzw. die große-Sieb-Ungleichung, die man zum Beweis des großen Siebes benötigt.

18.2. Satz vom großen Sieb: Sei $\mathcal{A} = (a_n)_{n \le N}$ eine Folge in $\mathbb{C}$, $w(p)$ die Anzahl der Streichungsresthklassen mod p, d.h. $w(p) := \#\{h(p);\ n \equiv h(p) \Rightarrow a_n = 0\}$, und sei $w(p) < p$ für alle $p \in \mathbb{P}$. Setze $g_w(q) := \mu^2(q) \prod_{\substack{p \mid q \\ p \in \mathbb{P}}} \frac{w(p)}{p - w(p)}$ und $L_w := \sum_{q \le Q} g_w(q)$ für $Q \ge 1$ beliebig. Dann ist

$$\Big|\sum_{n \le N} a_n\Big|^2 \le \frac{N + Q^2}{L_w} \sum_{n \le N} |a_n|^2.$$

Der Beweis des großen Siebs benötigt Exponentialsummen-Methoden.
Weiter zeigen wir den Satz nur mit "$\ll$" statt "$\le$" (ausreichend für alle hier vorgestellten Anwendungen).
Benötigt wird:

18.3. Die Große-Sieb-Ungleichung: Sei $(a_n)_{n \in \mathbb{N}} \subseteq \mathbb{C}$, $N, Q \ge 1$. Dann ist

$$\sum_{q \le Q} \sum_{\substack{a \bmod q \\ (a,q)=1}} \Big|\sum_{n \le N} a_n e\left(\frac{an}{q}\right)\Big|^2 \ll (N + Q^2) \sum_{n \le N} |a_n|^2.$$

Beweis:

Sei $F: [0,1] \to \mathbb{C}$ stetig diff'bar, auf $\mathbb{R}$ mit Periode 1 fortgesetzt.
(Bei uns: Setze $F(\alpha) := \left(\sum_{n \le x} a_n e(\alpha n)\right)^2$, wo $\alpha \in \mathbb{R}$.) Sei $z \in \mathbb{N}$.
Betr. $q \le z$, $q \in \mathbb{N}$, $1 \le a \le q$, $(a,q) = 1$, $\alpha \in [0,1]$. Dann:

$$\int_{a/q}^{\alpha} F'(t)\,dt = F(\alpha) - F\left(\frac{a}{q}\right) \Rightarrow \left|F\left(\frac{a}{q}\right)\right| \le |F(\alpha)| + \int_{a/q}^{\alpha} |F'(t)|\,dt. \quad (*)$$

Für $\delta > 0$ betr. $I(\frac{a}{q}) := [\frac{a}{q} - \delta, \frac{a}{q} + \delta] \subseteq [0,1]$.

$(*) \Rightarrow \quad 2\delta |F(\frac{a}{q})| \leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + \int_{I(\frac{a}{q})} \int_{a/q}^{\alpha} |F'(t)| dt \, d\alpha$

Mit $\alpha \in I(\frac{a}{q})$, $t \in [\frac{a}{q}, \alpha]$ folgt $t \in I(\frac{a}{q})$, also ist dies

$$\leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + \int_{I(\frac{a}{q})} \int_{I(\frac{a}{q})} |F'(t)| dt \, d\alpha,$$

also $\quad 2\delta |F(\frac{a}{q})| \leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + 2\delta \int_{I(\frac{a}{q})} |F'(\alpha)| d\alpha, \qquad \boxtimes$

wähle nun $\delta := \frac{1}{2z^2}$, so dass die Intervalle $I(a/q)$ für $q \leq z$ nicht überlappen (mod 1).

⌈Wäre sonst $x \in I(\frac{a}{q}) \cap I(\frac{a'}{q'})$ mit $\frac{a}{q} \neq \frac{a'}{q'}$, folgte $|\frac{a}{q} - \frac{a'}{q'}| \leq |\frac{a}{q} - x| + |x - \frac{a'}{q'}| < 2\delta = \frac{1}{z^2}$ $\oplus$

haben aber $|\frac{a}{q} - \frac{a'}{q'}| = \frac{|aq' - a'q|}{qq'} \neq 0$, also $\geq \frac{1}{qq'} \geq z^2$ im ↯ zu $\oplus$.⌋

Summation von $\boxtimes$ über alle IVe zeigt: $\frac{1}{z^2} \sum_{q \leq z} \sum_{\substack{a (q) \\ (a,q)=1}} |F(\frac{a}{q})| \leq \int_0^1 |F(\alpha)| d\alpha + \frac{1}{z^2} \int_0^1 |F'(\alpha)| d\alpha.$

Jetzt: $F(\alpha) = S(\alpha)^2$ mit $S(\alpha) = \sum_{n \leq x} a_n e(\alpha n)$, und $F'(\alpha) = 2 S(\alpha) S'(\alpha)$

zeigt $\sum_{q \leq z} \sum_{a(q), (a,q)=1} |S(\frac{a}{q})|^2 \leq z^2 \int_0^1 |S(\alpha)|^2 d\alpha + 2 \int_0^1 |S(\alpha) S'(\alpha)| d\alpha.$

Mit der Parsevalschen Gleichung $\int_0^1 |\sum_{n \leq x} a_n e(\alpha n)|^2 d\alpha = \sum_{n \leq x} |a_n|^2$

folgt nun $\int_0^1 |S(\alpha)|^2 d\alpha = \sum_{n \leq x} |a_n|^2$,

und haben $\int_0^1 |S(\alpha) S'(\alpha)| d\alpha \overset{C-S}{\leq} \left(\int_0^1 |S(\alpha)|^2 d\alpha\right)^{\frac{1}{2}} \left(\int_0^1 |S'(\alpha)|^2 d\alpha\right)^{\frac{1}{2}}$

$$\leq \left(\sum_{n \leq x} |a_n|^2\right)^{1/2} \cdot \left(\sum_{n \leq x} 4\pi^2 n^2 |a_n|^2\right)^{1/2} \leq 2\pi x \sum_{n \leq x} |a_n|^2.$$

Es folgt

$$\sum_{q \leq z} \sum_{a(q), (a,q)=1} |S(\frac{a}{q})|^2 \ll (z^2 + x) \sum_{n \leq x} |a_n|^2.$$ Jetzt: $Q = z$, $x = N$. $\square$

18.4. Bew. von Satz 18.2 (mit $\ll$ statt $\le$):

Sei $S(\alpha) = \sum_{n\le N} a_n e(\alpha n)$. Setze $Z(p,h) = \sum_{\substack{n\equiv h(p)\\ n\le N}} a_n$, $Z = \sum_{n\le N} a_n = S(0)$.

Dann ist für $p\in\mathcal{P}$:

$$\sum_{a=1}^{p} |S(\tfrac{a}{p})|^2 = \sum_{a=1}^{p}\sum_{n,m\le N} a_n\bar{a}_m e(\tfrac{a}{p}(n-m)) = p\sum_{\substack{n,m\le N\\ n\equiv m(p)}} a_n\bar{a}_m = p\sum_{h=1}^{p}|Z(p,h)|^2.$$

Die Subtraktion von $|S(0)|^2 = |Z|^2$ zeigt

$$\sum_{a=1}^{p-1}|S(\tfrac{a}{p})|^2 = p\sum_{h=1}^{p}|Z(p,h)|^2 - |Z|^2. \qquad (\times)$$

Für eine Streichungsrestklasse ist $Z(p,h)=0$, es folgt mit der Cauchy-Schwarz-Unglg.

$$|Z|^2 = \Big|\sum_{\substack{h\le p\\ Z(p,h)\neq 0}} Z(p,h)\Big| \underset{C\text{-}S}{\le} \Big(\sum_{\substack{h\le p\\ Z(p,h)\neq 0}} 1\Big)\cdot\Big(\sum_{h\le p}|Z(p,h)|^2\Big) = (p-w(p))\sum_{h\le p}|Z(p,h)|^2.$$

In $(\times)$ einsetzen: $\sum_{a=1}^{p-1}|S(\frac{a}{p})|^2 \ge \left(\frac{p}{p-w(p)}-1\right)|Z|^2 = \frac{w(p)}{p-w(p)}|S(0)|^2$.

Damit ist die Unglg. $\sum_{\substack{a\le p\\ (a,p)=1}} |S(\frac{a}{p})|^2 \ge \underbrace{\frac{w(p)}{p-w(p)}}_{=g_w(p)}\Big|\sum_{n\le N} a_n\Big|^2$ gezeigt.

Wegen dem Faktor $\mu^2(q)$ in $g_w(q)$ brauchen nur quadratfreie $q\le Q$ betrachtet werden.

Angenommen, für q und $\tilde{q}\le Q$, wo $(q,\tilde{q})=1$, sei $\sum_{\substack{a(q)\\ (a,q)=1}} |S(\frac{a}{q})|^2 \ge |S(0)|^2 g_w(q)$ $\oplus$ schon gezeigt.

Es folgt $\sum_{\substack{c\le q\tilde{q}\\ (c,q\tilde{q})=1}} |S(\frac{c}{q\tilde{q}})|^2 = \sum_{\substack{a\le q\\ (a,q)=1}}\sum_{\substack{b\le\tilde{q}\\ (b,\tilde{q})=1}} \underbrace{|S(\frac{a}{q}+\frac{b}{\tilde{q}})|^2}_{=\sum_n \underbrace{a_n e(n\frac{a}{q})}_{\text{neue } \tilde{a}_n}\cdot e(n\frac{b}{\tilde{q}}) = \tilde{S}(\frac{b}{\tilde{q}})} \ge g_w(\tilde{q})\sum_{\substack{a\le q\\ (a,q)=1}}|S(\frac{a}{q})|^2 \ge g_w(q\tilde{q})\cdot|S(0)|^2,$

$(q,\tilde{q})=1$ $\qquad$ g_w mult.

also folgt $\oplus$ für alle quadratfreien $q\le Q$.

Dies zeigt $\sum_{q\le Q}|S(0)|^2\cdot g_w(q) \le \sum_{q\le Q}\sum_{\substack{a(q)\\ (a,q)=1}}|S(\frac{a}{q})|^2$.

Mit der großen Sieb-Unglg. 18.3 für $q\le Q$ folgt nun die Beh. durch Auflösen nach $|S(0)|^2 = |\sum_{n\le N} a_n|^2$. $\square$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a19: Der Satz von Brun-Titchmarsh

Stichworte: Primzahlen in Progressionen und kurzen Intervallen, Satz von Brun-Titchmarsh, Beweis mit großem Sieb

---

19.1. Einleitung:
Die Zählfunktionen von Pzen lassen sich auf Progressionen verallgemeinern.
Eine etwas andere, aber oft verwandte Verallgemeinerung sind die Zählfunktionen auf kurzen Intervallen $]x, x+y] \subseteq \mathbb{R}$, das man "kurz" nennt, falls $y = o(x)$ gilt.

19.2. Def.: $\pi(x,y) := \pi(x+y) - \pi(x)$, $\vartheta(x,y) := \vartheta(x+y) - \vartheta(x)$, $\psi(x,y) := \psi(x+y) - \psi(x)$.
Eine Kombination ist auch möglich: So ist $\pi(x+y; q, a) - \pi(x; q, a)$ etwa die Anzahl der Pzen $p \equiv a (q)$ mit $p \in]x, x+y]$.
Im Hinblick auf den PZS müsste $\pi(x+y) - \pi(x) \sim \frac{x+y}{\log(x+y)} - \frac{x}{\log(x)} \approx \frac{y}{\log x}$ gelten, was aber selbst unter Ann. der (RH) nur für $y \gg \sqrt{x}$ folgt, und für sehr kleine y falsch ist.
Mit dem großen Sieb konnten [Montgomery/Vaughan, 1973] folgenden Satz zeigen:

19.3. Brun-Titchmarsh-Ungleichung: Seien $a, q \in \mathbb{N}$, $(a,q) = 1$, $x, y > 0$ reell. Dann:

$$q < y \Rightarrow \quad \pi(x+y; q, a) - \pi(x; q, a) < \frac{2y}{\varphi(q) \log(\frac{y}{q})}.$$

19.4. Bem.: • Speziell $x = 1$, schreibe wieder x für y: $\pi(x; q, a) < \frac{2x}{\varphi(q) \log(\frac{x}{q})}$.
Der Satz geht deutlich über den Siegel-Walfisz-Bereich $q \ll \log^A x$ hinaus, selbst unter (GRH), d.h. $\pi(x; q, a) = \frac{li(x)}{\varphi(q)} + O(\sqrt{x} \log x)$ kann dies nur mit $q \ll x^{1/2 - \varepsilon}$ gezeigt werden.
• Speziell $q = 1$: $\pi(x+y) - \pi(x) < \frac{2y}{\log y}$ für $y \geq y_0$ ist eine nichttriv. Absch., die so nicht mit dem PZS gewonnen werden kann.
• Der Faktor 2 spielt eine große Rolle im Zusammenhang mit Siegel-Nullstellen: [Motohashi, 1979] zeigte, dass wenn $\pi(x, q, a) \leq \frac{(2-\varepsilon)x}{\varphi(q) \log(\frac{x}{q})}$ gezeigt werden könnte mit einem $x \geq q^{c_0}$ und $\varepsilon > 0$, dann wäre $\beta \leq 1 - \frac{c\varepsilon}{\log(q)}$ für die Siegel-Nullstelle β, und ein $c > 0$.
Da laut Satz von Siegel aber $1 - \frac{c_n}{\log q} \leq \beta \leq 1$ gilt, folgt ein ↯, d.h. die Nichtexistenz von β. Eine Verbesserung von 2 auf $2 - \varepsilon$ wirkt sich also auf Siegel-Nullstellen aus.

Der Beweis von Satz 19.3 ist etwas aufwändig, wir zeigen mit unserem großen-Sieb-Satz hier nur die folgende, leicht schwächere Version:

19.5. **Brun-Titchmarsh-Ungleichung (einfacher):** Seien $a, q \in \mathbb{N}$, $(a,q)=1$, $x, y > 0$ reell. Dann:

$$q < y \Rightarrow \quad \pi(x+y; q, a) - \pi(x; q, a) \ll \frac{y}{\varphi(q)\log\left(\frac{y}{q}\right)}.$$

19.6. Beweis von 19.5: Betr. das Sieb $\mathcal{A} = \left]\frac{x-a}{q}, \frac{x+y-a}{q}\right] \cap \mathbb{Z}$, für $Q > 1$ betr. $\mathcal{P} = \{p \le Q;\ p \nmid q\}$, und gestrichen werde nur mit der Streichungsrestklasse $-aq^* \bmod p$ für jedes $p \in \mathcal{P}$, wobei $q^* \bmod p$ die inverse Restkl. von $q \bmod p$ sei, d.h. $qq^* \equiv 1\ (p)$. Sei nun $\tilde{p}$ eine PZ mit $x < \tilde{p} \le x+y$, $\tilde{p} \equiv a\ (q)$. Diese hat genau eine Darstellung $\tilde{p} = a + qn$ und $n \in \mathcal{A}$.
Ist $\tilde{p} > Q$, dann ist $qn \not\equiv -a \bmod p$ für alle $p \in \mathcal{P}$, also ist n Element der gesiebten Menge.
Mit $N := \frac{y}{q}$, $Q := \sqrt{N} > 1$ und $w(p) = 1$ für $p \in \mathcal{P}$ (es liegt ein kleines Sieb vor!) folgt

$$\pi(x+y; q, a) - \pi(x; q, a) \le \pi(Q) + S(\mathcal{A}, \mathcal{P}, Q) \le Q + \frac{N}{L_w} = Q + \frac{y}{qL_w}$$

wo $L_w = \sum_{\substack{d \le Q \\ (d,q)=1}} \mu^2(d) \prod_{p \mid d} \frac{1}{p-1} = \sum_{\substack{d \le Q \\ (d,q)=1}} \frac{\mu^2(d)}{\varphi(d)} \ge \frac{\varphi(q)}{q} \sum_{d \le Q} \frac{\mu^2(d)}{\varphi(d)}$,

denn $\frac{q}{\varphi(q)} = \prod_{p \mid q} \frac{p}{p-1} = \prod_{p \mid q}\left(1 + \frac{1}{p-1}\right) = \sum_{r \mid q} \frac{\mu^2(r)}{\varphi(r)} \Rightarrow \frac{q}{\varphi(q)} \sum_{\substack{d \le Q \\ (d,q)=1}} \frac{\mu^2(d)}{\varphi(d)} = \sum_{\substack{d \le Q \\ (d,q)=1}} \sum_{r \mid q} \frac{\mu^2(rd)}{\varphi(rd)} \ge \sum_{m \le Q} \frac{\mu^2(m)}{\varphi(m)}$.

die $m \le Q$, die qn'frei sind, sind schreibbar als $m = rd$, $r \mid q$, $(d,q)=1$

Nun ist auch $\frac{q}{\varphi(q)} = \prod_{p \mid q} \frac{1}{1 - \frac{1}{p}} = \prod_{p \mid q} \sum_{k \ge 0} \left(\frac{1}{p}\right)^k = \sum_{\substack{p \mid d \\ \Rightarrow p \mid q}} \frac{1}{d}$,

also $\sum_{m \le Q} \frac{\mu^2(m)}{\varphi(m)} = \sum_{m \le Q} \frac{\mu^2(m)}{m} \cdot \frac{m}{\varphi(m)} = \sum_{m \le Q} \frac{\mu^2(m)}{m} \cdot \sum_{\substack{p \mid d \\ \Rightarrow p \mid m}} \frac{1}{d} \ge \sum_{m \le Q} \frac{1}{m}$,

denn jedes $m \le Q$ ist schreibbar als $m = nd$, wo n qn'frei und $p \mid d \Rightarrow p \mid n$.
Also ist $L_w \ge \frac{\varphi(q)}{q} \cdot \sum_{m \le Q} \frac{1}{m} \gg \frac{\varphi(q)}{q} \log Q \gg \frac{\varphi(q)}{q} \log\left(\frac{y}{q}\right)$,
und als o.g. im Satz

erhalten wir $\ll \sqrt{\frac{y}{q}} + \frac{y}{q \frac{\varphi(q)}{q} \log\left(\frac{y}{q}\right)} \ll \frac{y}{\varphi(q) \log\left(\frac{y}{q}\right)}$, wie behauptet. $\square$

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a20: Abschätzung der PZ-Zwillingszählfunktion

Stichworte: PZ-Zwillingssieb für $\pi_2(x)$, o.S. für $\pi_2(x)$, Kleine-PZlücken-Problem, GPY, Prim-k-Tupel-Vermutung (DHL), große-PZlücken-Problem

---

20.1. Einleitung: Hatten $\pi_2(x) := \#\{p \le x;\ p+2 \in \mathbb{P}\}$ als Anzahl der PZ-Zwillinge in 17.10 eingeführt. Wir zeigen mit dem großen Sieb eine nichttriv. obere Abschätzung für $\pi_2(x)$. Es werden Neuerungen im Kleine- und große-PZlücken-Problem erläutert.

20.2. Def.: Das PZ-Zwillingssieb wird erklärt für $Q \le \sqrt{x}+3$ durch

$$\mathcal{A} :=]\sqrt{x}, x] \cap \mathbb{Z},\quad \mathcal{P} := \{p \le Q\},\quad W_p := \{0,-2\},\quad \text{insb. } w(p) = \#W_p = 2.$$

Die gesiebte Menge $S(\mathcal{A},\mathcal{P},Q) := \{n \in \mathcal{A};\ n(p) \notin W_p \text{ für alle } p \in \mathcal{P}\}$

$$= \{n \in \mathcal{A};\ (n(n+2), \prod_{p \le Q} p) = 1\} \quad (\text{vgl. Bsp. } 17.7)$$

besteht dann aus genau den PZen $p' \in]\sqrt{x}, x]$, für die $p'+2$ auch prim ist, sofern $Q > \sqrt{x}+2$ ist.

20.3. Folgerung: Der Satz 17.24 vom großen Sieb liefert

$$\pi_2(x) - \pi_2(\sqrt{x}) \ll (x + Q^2) \cdot \Big(\sum_{q \le Q} g(q)\Big)^{-1}$$

mit $g(q) = \mu^2(q) \prod_{p \mid q} \frac{w(p)}{p - w(p)}$, wobei

$$w(2) = 1,\quad w(p) = 2 \text{ für } p \ge 3 \text{ ist.}$$

Zum Auffinden einer u.S. für $g(q)$ wird g in geeigneter Weise als Faktung geschrieben.

20.4. Lemma: Sei $\omega(q) := \#\{p \mid q\}$ die Anzahl der (versch.) Primteiler von q. Dann gilt für $g(q)$ aus 20.3, dass durch $g(q) = 2^{\omega} * v(q)$ eine multipl. Fkt. v def. wird, für die gilt: $v(2) = 0$, $v(2^k) = 2\cdot(-1)^{k-1}$ für $k \ge 2$, $v(p) = \frac{4}{p-2}$ für $p \ge 3$, $v(p^k) = 2\cdot(-1)^{k-1}\frac{p+2}{p-2}$ für $p \ge 3$, $k \ge 2$.

Bew.:

• Für $p \geq 3$ bestätigt $\frac{2p}{p-2} = pg(p) = 2^{\omega} * v(p) = v(p)+2$ die Formel für $v(p)$, $\ulcorner v(p) = \frac{2p-2p+4}{p-2} \checkmark \lrcorner$

und für $k \geq 2$ gilt $g(p^k)=0$, so dass aus $0 = (2^{\omega} * v)(p^k) = v(p^k) + 2 \cdot \sum_{\ell=2}^{k-1} v(p^\ell) + 2 \cdot \underbrace{\left(\frac{4}{p-2}+1\right)}_{=\frac{p+2}{p-2}}$

mit einer Induktion über k die behaupteten Werte für $v(p^k)$ ergeben.

• Für $p=2$ geht man analog vor. $\ulcorner 2 \cdot \frac{1}{2^1} = 2 \cdot g(2) = 2^{\omega} * v(2) = 2^{\omega(1)} v(2) + 2^{\omega(2)} v(1) = v(2)+2 \Rightarrow v(2)=0 \checkmark$

$0 = (2^{\omega} * v)(2^k) = v(2^k) + 2 \cdot \sum_{\ell=2}^{k-1} v(2^\ell) + 2 \cdot (\underbrace{0}_{v(2)} + \underbrace{1}_{v(1)})$, VI $\lrcorner$ $\square$

20.5. Def.: Wir bilden die Dirichlet-Reihe $V(s) := \sum_{n \geq 1} \frac{v(n)}{n^s}$.

20.6. Lemma: $V(s)$ kgt. absolut in $\sigma > \frac{1}{2}$.

Bew.: Für $\sigma > \frac{1}{2}$ und jedes $N > 1$ gilt

$$\sum_{n \leq N} \left|\frac{v(n)}{n^s}\right| \leq \prod_{p \leq N} \left(1 + \sum_{a \geq 1} \frac{|v(p^a)|}{p^{a\sigma}}\right) \leq 7 \prod_{3 \leq p \leq N} \left(1 + \underbrace{\frac{4}{p^\sigma(p-2)}}_{(a=1)} + 10 \sum_{a \geq 2} p^{-a\sigma}\right)$$

$$\leq 7 \underbrace{\prod_{3 \leq p \leq N} \left(1 + \frac{c_1}{p^{\sigma+1}} + \frac{c_2}{p^{2\sigma}}\right)}_{\text{kgt. für } N \to \infty. \ (\sigma > \frac{1}{2})} \quad \text{für geeignete } c_1, c_2 > 0,$$

$\square$

20.7. Kor.: Für alle $\alpha > \frac{1}{2}$, $\varepsilon > 0$ gilt also

$$\sum_{n > N} \frac{|v(n)|}{n^\alpha} \ll N^{1/2 - \alpha + \varepsilon}. \quad \ulcorner \text{l.S.} = \sum_{n > N} \frac{|v(n)|}{n^{(\alpha - \frac{1}{2} - \varepsilon) + \frac{1}{2} + \varepsilon}} \ll N^{-\alpha + \frac{1}{2} + \varepsilon} \cdot \underbrace{\sum_{n \geq 1} \frac{|v(n)|}{n^{\frac{1}{2}+\varepsilon}}}_{\ll 1}. \lrcorner$$

20.8. Lemma: Es gilt $\sum_{q \leq Q} g(q) = \frac{1}{2\zeta(2)} V(1) \log^2(Q) + O(\log(Q))$.

Bew.: • Aus $qg(q) = 2^{\omega(d)} * v(q)$ folgt zunächst

$$\sum_{q \leq Q} g(q) = \sum_{d \leq Q} \frac{2^{\omega(d)}}{d} \sum_{r \leq Q/d} \frac{v(r)}{r} = \sum_{d \leq Q} \frac{2^{\omega(d)}}{d} \left(V(1) + O\left(\left(\frac{d}{Q}\right)^{1/4}\right)\right).$$

$(\varepsilon = \frac{1}{4})$ (mit Kor. 20.7)

• Aus $2^{\omega(q)} = \mathbb{1} * \mu^2$ folgt $\sum_{d \leq Q} \frac{2^{\omega(d)}}{d} = \sum_{n \leq Q} \frac{1}{n} \sum_{m \leq Q/n} \frac{\mu^2(m)}{m} =$

$\ulcorner$ l.S.$(p^a) = 1 + \mu^2(p) = 2$, l.S.$(p^a) = 2^1 \checkmark \lrcorner$

$$= \sum_{n \leq Q} \frac{1}{n} \left(\frac{1}{\zeta(2)} \cdot \log\left(\frac{Q}{n}\right) + O(1)\right) = \frac{1}{2\zeta(2)} \log^2(Q) + O(\log(Q)).$$

$\ulcorner \sum_{n \leq Q} \frac{1}{n} \log\left(\frac{Q}{n}\right) = \frac{1}{2} \log^2(Q) + O(\log(Q))$ $\ulcorner$ mit p.Σ. aus Asymptotik für $\sum_{r \leq x} \frac{1}{r}$ $\lrcorner$

$\ulcorner$ p.Σ aus $\mu^2(m) = \sum_{d^2 | m} \mu(d)$ und Asymptotik für $\sum_{r \leq x} \frac{1}{r}$,

nämlich $\sum_{r \leq x} \frac{1}{r} = \log(x) + \gamma + O\left(\frac{1}{x}\right)$ $\lrcorner$

- Wiederum p. Σ mit $f(x)=x^{1/4}$ liefert $\sum_{d\le Q}\frac{2^{\omega(d)}}{d^{3/4}}=O(Q^{1/4}\log(Q))$.
- Alles zusammen zeigt

$$\sum_{q\le Q} g(q)=\frac{1}{2\zeta(2)}V(1)\log^2(Q)+O(\log(Q)).$$ □

20.9. **Lemma:** $V(1)\neq 0$.

Bew.: Es ist $\frac{V(1)}{\zeta(2)}$ der Wert von $\frac{V(s)}{\zeta(2s)}=:\sum_{n\ge1}\frac{b(n)}{n^s}$ bei $s=1$.

Da $\frac{1}{\zeta(s)}=\sum_{n\ge1}\frac{\mu(n)}{n^s}$, folgt $\frac{1}{\zeta(2s)}=\sum_{m\ge1}\frac{a(m)}{m^s}$ mit $a(m):=\begin{cases}\mu(n), & \text{falls } \exists n: m=n^2,\\ 0, & m \text{ kein } \square.\end{cases}$

Es ist $b=a*v$,

also $b(n)=\sum_{d^2|n}\mu(d)\,v\left(\frac{n}{d^2}\right)$ und $b(p^k)=\begin{cases}v(p^k)-v(p^{k-2}), & \text{für } k\ge2,\\ v(p), & \text{für } k=1.\end{cases}$

Aus L. 20.4 folgt $b(p^k)=0$ für $k\ge4$, sowie $b(2)=0$, $b(4)=-3$, $b(8)=2$, und für $p\ge3$ ist $b(p)=\frac{4}{p-2}$, $b(p^2)=\frac{3p+2}{2-p}$, $b(p^3)=\frac{2p}{p-2}$.

Die Reihen für $\frac{1}{\zeta(2s)}$ und $V(s)$ konvergieren absolut für $\sigma>\frac12$, der Eulersche Π-Satz liefert die Produktentwicklung

$$\frac{V(1)}{\zeta(2)}=\prod_p\left(1+\frac{b(p)}{p}+\frac{b(p^2)}{p^2}+\frac{b(p^3)}{p^3}\right)=\frac12\prod_{p\ge3}\left(1+\frac{1}{p(p-2)}\right),$$

der Kehrwert ist

$$\frac{\zeta(2)}{V(1)}=2\prod_{p\ge2}\left(1-\frac{1}{(p-1)^2}\right)=:C_2'\neq0.$$ □

20.10. **Def.:** $C_2:=2\prod_{p\ge2}\left(1-\frac{1}{(p-1)^2}\right)$ heißt Zwillingskonstante (gelegentlich ohne Faktor 2), vgl. a17.9.

20.11. **Satz:** Für $x\to\infty$ gilt $\pi_2(x)\le 8C_2\frac{x}{\log^2(x)}+o\left(\frac{x}{\log^2(x)}\right)$.

Bew.: $\pi_2(x)-\pi_2(\sqrt{x})\underset{20.3}{\ll} x\cdot\left(\sum_{q\le Q}g(q)\right)^{-1}\underset{20.8}{\le}\frac{4\zeta(2)}{V(1)}\cdot\frac{x}{\log^2(x)}\rightsquigarrow\pi_2(x)\le 8\overbrace{\frac{\zeta(2)}{V(1)}}^{C_2}\cdot\frac{x}{\log^2(x)}$. □

$Q=\sqrt{x}/\log(x)$, "$\le$" bei scharfem großen Siebe (für $Q=\sqrt{x}$ haben $x+Q^2\le 2x\rightsquigarrow$ Faktor 2 mehr.)

20.12 **Bem.:**
- Damit sind die Kor. 17.12/13 gezeigt.
- Laut der Vermutung von Hardy und Littlewood, $\pi_2(x)\sim C_2\frac{x}{\log^2(x)}$ (vgl. a17.9) gilt aber vermutlich viel mehr.

Unter Ann. der (GRH) haben H&L. dies gezeigt.

• [Heath-Brown, 1983] zeigte: Falls es Siegel-Nst. (vgl. a11.4) gibt, dann ex. ∞ viele PZ-Zwillinge $p, p+2$.

Für den Rest dieses Kapitels gelte: Wir numerieren die Folge der PZen aufsteigend: $p_1 = 2 < p_2 = 3 < p_3 = 5 < \dots$, d.h. p_n sei die n-te PZ.

20.13. Beh.: Es gilt $p_n \sim n \log(n)$ für $n \to \infty$. ⌐ Ü Blatt 4 Aufgabe 2 ⌙

Vor Kurzem hat sich ein neuer Zugang zur PZ-Zwillingsvermutung eröffnet, der mit dem Studium von PZ-Lücken arbeitet.

20.14. Def.: Die Zahl $d_n := p_{n+1} - p_n$ heißt n-te PZ-Lücke.

20.15 Kleines PZ-Lückenproblem: Wie klein ist die kleinste PZ-Lücke, die ∞ oft vorkommt? (Diese ist 2, falls die PZ-Zwillingsvermutung wahr ist.)
Anders ausgedrückt: Finde eine o.S. für $\liminf_{n\to\infty}(d_n)$.
Erwartungsgemäß ist $d_n \sim \log(p_n)$ mit der plausiblen Ann. $\log(p_{n+1}) \sim \log(p_n)$, denn $(n+1)\log(p_n) - n\log(p_n) = \log(p_n)$ und 20.13.
Lange Zeit war unbekannt, ob $\log(p_n)$ überhaupt unendlich oft unterschritten wird, oder ob gar eine Konstante als o.S. für $\liminf_{n\to\infty}(d_n)$ beweisbar ist.
Dies wurde erst vor kurzem bestätigt und als großer Durchbruch gefeiert.

20.16 Satz von GPY [Goldston, Pintz, Y, Idiram 2007]: $\liminf_{n\to\infty} \frac{d_n}{(\log(p_n))^{1/2}(\log\log(p_n))^2} < \infty$,
insb. ist unendlich oft $d_n < \sqrt{\log(p_n)}(\log\log(p_n))^2 = o(\log(p_n))$.
Dazu wurde eine neue Siebmethode eingeführt, heute bekannt als GPY-Sieb.

20.17. Satz von Zhang, 2013: $\liminf_{n\to\infty}(d_n) \leq 70.000.000$.
Der Beweis erfordert neben dem GPY-Sieb umfangreiche neue Abschätzungen von sog. Kloosterman-Summen, das sind spezielle Exponentialsummen der Form $K(a,b;m) := \sum_{\substack{1\leq x<m \\ (x,m)=1}} e\left(\frac{ax+bx^*}{m}\right)$, wo $xx^* \equiv 1 \ (m)$.

20.18. Satz von Maynard / Tao, 2013: $\liminf_{n\to\infty}(d_n) \leq 600$.
Der Beweis benutzt neben der GPY-Sieb-Idee eine "multidim." Variante des Selberg-Siebs. Der Beweis ist einfacher als der von Zhang und numerisch besser.

20.19. Satz [Polymath 8b, 2013]: $\liminf_{n\to\infty}(d_n) \leq 246$.
Durch Kombination aller verfügbaren Methoden und möglichst genauer effektiver Bestimmung aller vorkommenden Konstanten gelang dieses Gemeinschaftsprojekt.
Dabei entstand auch das folgende Ergebnis:
Satz: $(EH) \Rightarrow \liminf_{n\to\infty}(d_n) \leq 12$, $(GEH) \Rightarrow \liminf_{n\to\infty}(d_n) \leq 6$.
Hier steht (EH) für eine zur (GRH) verwandte Aussage genannt Elliott-Halberstam-Vermutung, und (GEH) für eine plausible Verallgemeinerung davon. Mit den bislang bekannten Methoden sind weitere numerische Verbesserungen ausgeschlossen.

Anhang:
Wir erläutern die Grundidee des GPY-Siebs:

Wir verallgemeinern das Konzept "Primzahlzwilling" $p, p+2h \in \mathbb{P}$ zunächst zu einem "Primzahldetektor", bei dem auch PZ Drillinge, PZ Vierlinge usw. betrachtet werden sollen. Bei Drillingen ist die Konstellation $p, p+2, p+4$ ungünstig, da eine der drei Zahlen stets durch 3 teilbar ist, da $(0,2,4)$ alle Reste mod 3 abdeckt. Eine solche Konstellation, wie geg. durch das Tripel $(0,2,4)$, nennt man unzulässig. Bei Paaren ist $(0,1)$ unzulässig, bei Vierlingen ist z.B. $(0,1,3,6)$ unzulässig, usw.

20.20. Def.: Ein Tupel $\underline{h} \in \mathbb{N}_0^k$ heißt zulässig, falls $\forall p \in \mathbb{P}: \#\{h_i \bmod p;\ 1 \leq i \leq k\} < p$.
Dann erwarten wir, dass unendlich oft Primzahltupel damit erzeugt werden:

20.21. Prim-k-Tupel-Vermutung: Sei $\underline{h} \in \mathbb{N}_0^k$ ein zulässiges k-Tupel. Dann gibt es unendlich viele $n \in \mathbb{N}$, so dass $n + \underline{h} := (n+h_1, n+h_2, \ldots, n+h_k) \in \mathbb{P}^k$.
Die Prim-k-Tupel-Vermutung ist auch als Dickson-Hardy-Littlewood-Vermutung (DHL) bekannt.

20.22. Die GPY-Idee besteht nun darin, nachzuweisen, dass für ein zulässiges Tupel unendlich oft irgend zwei der Komponenten von $n+h_j$ PZen sind, wenn $n\to\infty$, etwa durch einen Schubfachschluss.

Dazu sei $\theta(n) := \begin{cases} \log n, & n \text{ prim}, \\ 0, & \text{sonst}, \end{cases}$

für $x>1$ groß setze $S_1(x) := \sum_{x\le n<2x} w(n)$, $S_2(x) := \sum_{x\le n<2x} \left(\sum_{j=1}^{k} \theta(n+h_j)\right) w(n)$.

Die Funktion $w : [x, 2x] \cap \mathbb{N} \to \mathbb{R}_{>0}$ wird geschickt gewählt. Lässt sich nun zeigen, dass $S_2(x) > S_1(x)\log(3x)$ für alle $x \ge x_0$, dann folgt für ein $n\in[x,2x[$, dass $\sum_{j=1}^{k}\theta(n+h_j) > \log(3x)$ ist. ⌜Sonst wäre $S_2(x) \le \log(3x) S_1(x)$⌟. Dann müssen (Schubfachschluss!) mindestens zwei der $n+h_j$ Primzahlen sein, welche den Abstand $\le \max_{1\le i\ne j\le k} |h_i - h_j| =: H$ haben. Gilt dies für alle hinreichend großen x, schlägt der "Test" auf PZabstände $\le H$ also unendlich oft an. Auch benachbarte PZpaare haben dann unendlich oft höchstens diesen Abstand.

Dies gelang GPY mit folgender Wahl für w:

$$w(n) := \Big(\sum_{\substack{d\le D\\ d\mid P(n)}} \lambda(d)\Big)^2, \text{ wo } \lambda(d) = \mu(d)\log\left(\frac{D}{d}\right)^{k+l} \text{ mit } l \approx \sqrt{k},$$

$$D = x^{\alpha} \text{ und } P(n) := \prod_{j=1}^{k}(n+h_j).$$

Diese "Gewichtsfunktion" $w(n)$ ist durch das Selberg-Sieb motiviert.

Die Berechnung von $S_2(x)$ ergibt mit diesem $w(n)$ den Ausdruck

$$S_2(x) = \sum_{d_1,d_2\le D} \lambda(d_1)\lambda(d_2) \sum_{\substack{n,\ x\le n<2x\\ \operatorname{ggT}(d_1,d_2)\mid P(n)}} \sum_{j\le k} \theta(n+h_j).$$

Die Bedingung $\operatorname{kgV}(d_1,d_2) \mid (n+h_1)\cdots(n+h_k)$ so, dass $n+h_1,\dots,n+h_k \in \mathbb{P}$, zeigt, dass laut Chinesischem Restsatz PZen in bestimmten Restklassen mod $\operatorname{kgV}(d_1,d_2)$ gezählt werden müssen. GPY haben gezeigt, dass dies zur Lösung des kleinen PZlückenproblems führt.

20.23. <u>Verbesserung von Maynard/Tao des GPY-Siebs:</u>
Ändere w ab in $w(n) = \left(\sum_{\substack{d_1,\dots,d_k \le D \\ d_i \mid n+h_i,\, \forall i}} \mu(d_1\cdots d_k)\, G\left(\log\left(\frac{D}{d_1\cdots d_k}\right)\right) \right)^2$,

G geeignet.

Diese Gewichtsfunktion kann als die einer mehrdimensionalen Variante des Selberg-Siebs gedeutet werden, bei der die Bedingung $d_i \mid n+h_i$ individuell für jedes i angesetzt wird. Dies ermöglicht mehr Freiraum in der Methodik und führt somit zu numerischen Verbesserungen.

20.24 Eng verwandt mit dem kleinen Primzahllückenproblem ist das <u>Große Primzahllückenproblem:</u> Zeige dass von $d_n = p_{n+1} - p_n$ die Größe $\log(p_n)$ unendlich oft deutlich überschritten wird.
In folgender Form konnten Erdős und Rankin dies 1938 beweisen:

20.25 <u>Satz von Erdős-Rankin:</u> Es gibt ein $C>0$, so dass für unendl. viele n gilt:

$$d_n \geq C \log(p_n) \cdot \underbrace{\frac{\log\log(p_n)}{(\log\log\log(p_n))^2} \cdot \log\log\log\log(p_n)}_{\text{div. für } n\to\infty}$$

Erdős hielt eine Verbesserung dieses Satzes seinerzeit für ein schwieriges und herausforderndes Problem. Er vermutete, dass die Konstante $C>0$ zu einer divergenten Funktion verbessert werden können müsste. Bis 2014 werden hingegen nur numerische Verbesserungen der Konstanten $C>0$ erreicht (etwa 1963 von Rankin, der $C = e^{\sigma}$ zeigte).

Erdős war bekannt dafür, für bestimmte Probleme, die unlösbar erschienen, (kleinere) Geldpreise auszusetzen. Das Erdős-Rankin-Problem hatte er mit der höchsten Summe von 10.000 $ ausgelobt.

Im Jahr 2014 gab Maynard auf arxiv.org eine Lösung bekannt, und ebenso in derselben Woche die Mathematiker Ford, Konyagin, Green und Tao.
Inzwischen ist die folgende, bislang beste Version, bekannt, die mit den aktuellen Methoden wohl kaum weiter verbessert werden kann:

2026. Satz von Maynard-Ford-Konyagin-Green-Tao (2018): Es ex. $C>0$, so dass für unendlich viele n gilt: $d_n \geq C \cdot \log(n) \cdot \frac{\log\log(n)\,\log\log\log\log(n)}{\log\log\log(n)}$.

Der Exponent 2 hier ist getilgt!
Die Methoden/Verbesserungen stammen aus den Durchbrüchen im kleinen Primzahlensatz, d.h. die mehrdim. Selberg-Siebe-Gewichte in 2023 spielen darin eine wesentliche Rolle.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a21: Der Satz von Bombieri-Vinogradov

Stichworte: Große-Sieb-Ungleichung für Charaktersummen, Vaughans Identität, Satz von Bombieri-Vinogradov, level of distribution, Elliott-Halberstam-Vermutung

---

21.1. Einleitung: Wir zeigen den Satz von Bombieri-Vinogradov, der Beweis folgt modernen Methoden. Benötigt wird die große-Sieb-Ungleichung für (bilineare) Charaktersummen, sowie die Vaughan-Identität als eine Art kombinatorisches Hilfsmittel. Der Gültigkeitsbereich des Satzes von B-V liefert den level of distribution.

21.2. Satz (Das große Sieb für Charaktersummen): Seien $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{C}$. Dann:

(i) $$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}\Big|\sum_{n=M}^{M+N}a_n\chi(n)\Big|^2 \le (N+Q^2)\sum_{n=M}^{M+N}|a_n|^2$$

(ii) $$\sum_{R<q\le Q}\frac{1}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}\Big|\sum_{n=M}^{M+N}a_n\chi(n)\Big|^2 \le \Big(\frac{N}{R}+Q\Big)\sum_{n=M}^{M+N}|a_n|^2,$$

$\uparrow$ alle primitiven χ mod q wo $R, Q, M, N \ge 1$.

Bew.:

Haben $$\Big|\sum_n a_n\chi(n)\Big|^2 = \frac{1}{q}\Big|\sum_{a=1}^{q}\sum_n \bar\chi(a)e\Big(\frac{an}{q}\Big)a_n\Big|^2,$$

da $\bar\chi(n)\tau(\chi) = \sum_{a(q)}\chi(a)e\big(\frac{an}{q}\big)$ laut Beweisende von L. 12.8, mit $|\tau(\chi)|^2 = q$

Summation über χ zeigt $$\sideset{}{^*}\sum_{\chi(q)}\Big|\sum_n a_n\chi(n)\Big|^2 \le \frac{1}{q}\sum_{\chi(q)}\Big|\sum_{a=1}^{q}\sum_n\bar\chi(a)e\Big(\frac{an}{q}\Big)a_n\Big|^2$$

$$= \frac{1}{q}\sum_{a,b=1}^{q}\sum_{m,n}\sum_{\chi(q)}\bar\chi(a)\chi(b)e\Big(\frac{an-bm}{q}\Big)a_n\overline{a_m}$$

$$\overset{\text{OMR}}{=} \frac{\varphi(q)}{q}\sideset{}{^*}\sum_{a(q)}\sum_{m,n}e\Big(\frac{a(n-m)}{q}\Big)a_n\overline{a_m} = \frac{\varphi(q)}{q}\sideset{}{^*}\sum_{a(q)}\Big|S\Big(\frac{a}{q}\Big)\Big|^2,$$

wo $S(\alpha) := \sideset{}{^*}\sum_{a(q)} a_n e(\alpha n)$.

Die Anwendung der große-Sieb-Ungleichung 18.3 zeigt nun (i), und (ii) folgt aus (i) mit p. $\sum$ $\big(f(t)=\frac{1}{t}\big)$. □

21.3. **Bem.:** Direkt aus der C-S-Unglg. folgt damit

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}\Big|\sum_{m\le M}\sum_{n\le N}a_m b_n\chi(mn)\Big| \overset{C-S}{\ll} (M+Q^2)^{\frac12}(N+Q^2)^{\frac12}\Big(\sum_m|a_m|^2\Big)^{\frac12}\Big(\sum_n|b_n|^2\Big)^{\frac12},$$

wir benötigen aber eine leichte Abwandlung davon:

21.4. **Satz:** Für $(a_m)_{m\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}\subseteq\mathbb{C}$ gilt:

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}\max_X\Big|\sum_{\substack{m\le M,\ n\le N\\ m\cdot n\le X}}a_m b_n\chi(mn)\Big| \ll (M+Q^2)^{\frac12}(N+Q^2)^{\frac12}\Big(\sum_m|a_m|^2\Big)^{\frac12}\Big(\sum_n|b_n|^2\Big)^{\frac12}\cdot\log(2MN).$$

Der Beweis von 21.4 benötigt:

21.5. **Lemma:** Sei $T,\beta>0$, $\alpha\in\mathbb{R}$. Dann gilt: $\displaystyle\int_{-T}^{T}e^{it\alpha}\frac{\sin(t\beta)}{t}\,dt = \begin{cases}\pi+O\left(\frac{1}{T(\beta-|\alpha|)}\right), & |\alpha|<\beta,\\ O\left(\frac{1}{T(|\alpha|-\beta)}\right), & |\alpha|>\beta.\end{cases}$

Bew.: Die Beh. ist eine Variante der Perronschen Formel bzw. Lemma 3.11 und kann daraus durch sorgfältigen Grenzübergang für $c\to 0$ gefolgert werden. [Direkter Beweis auch möglich, vgl. [Brüdern, S. 186/187]] □

21.6. **Bew. von Satz 21.4:** • Da für $MN\le X$ die Bed. $mn\le X$ redundant ist, genügt es OE, das Maximum für $X\le MN$ zu erstrecken.

• Für $\gamma_m,\eta_n\in\mathbb{C}$ zeigt 21.5. mit $\beta=\log(X)$, $\alpha=\log(mn)$, dass

$$\sum_{\substack{m\le M,\ n\le N\\ mn\le X}}\gamma_m\eta_n = \int_{-T}^{T}\Big(\sum_{m\le M}\gamma_m m^{it}\Big)\Big(\sum_{n\le N}\eta_n n^{it}\Big)\frac{\sin(t\log(X))}{\pi t}\,dt + O\Big(\frac{1}{T}\sum_{\substack{m\le M\\ n\le N}}|\gamma_m\eta_n|\frac{1}{|\log(\frac{mn}{X})|}\Big).$$

Nimm OE $K=\lfloor X\rfloor+\frac12$, dann ist $\left|\frac{mn}{X}-1\right|\ge\frac{1}{2X}\Rightarrow\left|\log\left(\frac{mn}{X}\right)\right|\gg\frac{1}{X}\gg\frac{1}{MN}$ laut $MN\ge X$.

Die Abschätzung $\sin(t\log(X))\le\min(1,|t|\log(2MN))$ liefert

$$\sum_{\substack{m\le M,\ n\le N\\ mn\le X}}\gamma_m\eta_n \ll \int_{-T}^{T}\Big|\sum_{m\le M}\gamma_m m^{it}\sum_{n\le N}\eta_n n^{it}\Big|\min\Big(\frac{1}{|t|},\log(2MN)\Big)\,dt + \frac{MN}{T}\sum_{\substack{m\le M\\ n\le N}}|\gamma_m\eta_n|,$$

mit $\max\limits_{X\le MN}$ über die l.S. genommen, da r.S. unabh. von X.

• Setze $\gamma_m=a_m\chi(m)$, $\eta_n=b_n\chi(n)$, $U(t):=\min\left(\frac{1}{|t|},\log(2MN)\right)$,

$A(t,\chi):=\sum_{m\le M}a_m\chi(m)m^{it}$, $B(t,\chi):=\sum_{n\le N}a_n\chi(n)n^{it}$.

• Summation über χ und q ergibt dann

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}\max_{X\le MN}\Big|\sum_{\substack{m\le M\\ n\le N\\ mn\le X}} a_m b_n \chi(mn)\Big| \ll \int_{-T}^{T}\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi(q)}|A(t,\chi)B(t,\chi)|U(t)\,dt + \frac{Q^2MN}{T}\sum_{\substack{m\le M\\ n\le N}}|a_m b_n|$$

21.3 & C-S $\to$ mit $a'_m = a_m m^{it}$, $b'_n = b_n n^{it}$

$$\ll (M+Q^2)^{\frac12}(N+Q^2)^{\frac12}\Big(\sum|a_m|^2\Big)^{\frac12}\Big(\sum|b_n|^2\Big)^{\frac12}\int_{-T}^{T}U(t)\,dt + \frac{Q^2(MN)^{3/2}}{T}\Big(\sum_m|a_m|^2\Big)^{\frac12}\Big(\sum_n|b_n|^2\Big)^{\frac12},$$

Mit $T=(MN)^{3/2}$ folgt die Beh. □

Neben Satz 21.4 wird für den Beweis des Satzes von Bombieri-Vinogradov noch eine Summen-Identität benötigt.

21.7. **Lemma** (Vaughans Identität): Seien $U,V\ge 1$ und f eine zahlentheoretische Fkt.

Dann: $\sum_{n\le x}\Lambda(n)f(n) = S_1+S_2+S_3+S_4$ mit $S_i := \sum_{n\le x} a_i(n)f(n)$, $i=1,2,3,4$,

wobei $a_1(n) := \begin{cases}\Lambda(n), & n\le U,\\ 0, & n>U,\end{cases}$ $\quad a_3(n) := \sum_{kl=n,\ l\le V}\mu(l)\log(k)$,

$a_2(n) := -\sum_{klm=n,\ l\le U,\ m\le V}\Lambda(l)\mu(m)$, $\quad a_4(n) := -\sum_{mk=n,\ m>U,\ k>V}\Lambda(m)\sum_{d\mid k,\ d\le V}\mu(d)$.

Bew.: Sei $F(s) := \sum_{n\le U}\frac{\Lambda(n)}{n^s}$, $G(s) := \sum_{n\le V}\frac{\mu(n)}{n^s}$.

Koeff.vgl. der Glg. $-\frac{\zeta'}{\zeta}(s) = F(s) - \zeta(s)F(s)G(s) - \zeta'(s)G(s) + \left(-\frac{\zeta'}{\zeta}(s) - F(s)\right)(1-\zeta(s)G(s))$

ergibt $\Lambda(n) = a_1(n) + a_2(n) + a_3(n) + a_4(n)$,

dies noch mal $f(n)$ nehmen und $\sum_{n\le x}$ darüber zeigt die Beh. □

21.8 **Bem.:** Haben (i) $S_3 = \sum_{l\le V}\mu(l)\sum_{k\le x/l}f(kl)\int_1^k\frac{dy}{y} = \int_1^x\sum_{l\le V}\mu(l)\sum_{y<k\le x/l}f(kl)\frac{dy}{y}$

$$\ll \log(x)\sum_{l\le V}\max_w\Big|\sum_{w<k\le x/l}f(kl)\Big|.$$

(ii) In S_4 ist für $1\le k\le V$

die Glg. $\sum_{d\mid k,\ d\le V}\mu(d)=0$ zu beachten, es folgt also $k>V$ und

$$S_4 = -\sum_{U<m\le x/V}\ \sum_{V<k\le x/m}\Lambda(m)\beta(k)f(km), \quad \beta(k) := \sum_{d\mid k,\ d\le V}\mu(d).$$

(iii) Haben $S_2 = -\sum_{t\le UV} \alpha(t) \sum_{k\le x/t} f(kt)$ mit $\alpha(t) := \sum_{\substack{ml=t\\ m\le V, l\le U}} \Lambda(l)\mu(m)$.

Zerlegen $S_2 = S_5 + S_6$ mit Bed. $t\le U$ in S_5 und $U<t\le UV$ in S_6.
Dann kann S_5 wie bei S_3 abgeschätzt werden, da $\sum_{l|t}\Lambda(l) = \log(t)$, also $|\alpha(t)|\le \log(t)$
und $|S_5| \le \log(x) \sum_{l\le U} \max_w \left|\sum_{w<k\le x/l} f(kl)\right|$.

(iv) Für S_6 ergibt sich $S_6 = -\sum_{U<m\le UV} \sum_{k\le x/m} \alpha(m) f(km)$.

21.9. **Kor.:** Seien $U,V\ge 1$, $UV\le x$, f eine zth. Fkt. Dann gilt $\sum_{U<m\le x} f(m)\Lambda(m) \ll \log(x) T_1 + T_2 + T_3$
mit $T_1 := \sum_{l\le \max(U,V)} \max_w \left|\sum_{w<k\le x/l} f(kl)\right|$, $T_i := \left|\sum_{U<m\le \max(\frac{x}{V},UV)} \sum_{x\le \frac{a}{m}} a_i(m) b_i(k) f(mk)\right|$, $i=2,3$,
wo $a_i(m)$, $b_i(k)$ zth. Fktn. sind, die
nur von U,V abh. sind, für die $|b_i(k)| \le \sum_{t|k} 1$, $|a_i(k)|\le \log(k)$ für alle $k\in\mathbb{N}$ gelte.

Bew.: Setze $a_2(m) := \begin{cases}\Lambda(m), & m\le \frac{x}{V},\\ 0, & \text{sonst},\end{cases}$ $a_3(m) := \begin{cases}\alpha(m), & m\le UV\\ 0, & \text{sonst},\end{cases}$

$b_2(k) := \begin{cases}\beta(k), & \text{für } k>V,\\ 0, & \text{sonst},\end{cases}$ $b_3(k) := 1$.

Dann Lemma 21.7 mit Bem. 21.8: S_1, S_3, S_5 als T_1, S_4 als T_2, S_6 als T_3 abschätzen. □

Ohne Zerlegung von S_2 erhalten wir auch sofort:

21.10. **Kor.:** Seien $U,V\ge 1$, $UV\le x$, f eine zth. Fkt. Dann gilt $\sum_{U<m\le x} f(m)\Lambda(m) \ll \log(x) T_1' + T_2'$
mit $T_1' = \sum_{l\le UV} \max_w \left|\sum_{w<k\le x/l} f(kl)\right|$, $T_2' = \left|\sum_{U<m\le \frac{x}{V}} \sum_{V<k\le \frac{x}{m}} \Lambda(m) b(k) f(mk)\right|$
zth. Fkt., nur von V abh.
mit $|b(k)| \le \sum_{t|k} 1$.

Damit kommen wir zum Hauptergebnis, dazu eine Bezeichnung:

21.11. **Def.:** Für $q\in\mathbb{N}$, $(a,q)=1$, sei $E(x;q,a) := \psi(x;q,a) - \frac{x}{\varphi(q)}$
die Größe des Fehlerterms des PZS in APs, $p\equiv a\,(q)$,
(in der ψ-Version).

21.12. **Satz von Bombieri–Vinogradov [1966]**: Sei $A>1$, $Q\geq 1$. Dann gilt

$$\sum_{q\leq Q}\ \max_{(a,q)=1}\ \max_{y\leq x}|E(y;q,a)| \ll_A \frac{x}{\log^A(x)} + Q\sqrt{x}\cdot\log^6(Qx).$$

21.13. **Bem.**: • Für $Q\leq \frac{\sqrt{x}}{\log^{A+6}(x)}$ ist die r.S. dann $\ll_A \frac{x}{\log^A(x)}$.

• Die implizite Konstante hängt in nicht angebbarer Weise von A ab wegen der Verwendung des Satzes von Siegel–Walfisz 11.6.

Der wichtigste Schritt zum Beweis ist folgendes Hilfsmittel.

21.14. **Lemma (von Vaughan, auch: "Basic mean value theorem")**: Sei $x,Q\geq 1$. Dann:

$$\sum_{q\leq Q}\frac{q}{\varphi(q)}\sum_{\chi(q)}^{*}\max_{y\leq x}|\Psi(y,\chi)| \ll \left(x+x^{\frac{5}{6}}Q+\sqrt{x}Q^2\right)\cdot\log^5(Qx).$$

Bew.: Für $Q^2>x$ folgt die Beh. sofort aus Bem. 21.3, angewendet mit $M=1$, $N=x$, $a_1=1$, $b_m=\Lambda(m)$. Sei also $Q^2\leq x$.

Weiter sei $y=y(\chi)\leq x$ so, dass $|\Psi(y,\chi)|=\max_{z\leq x}|\Psi(z,\chi)|$.

Für $U,V\geq 1$ gemäß den Bed. in Kor. 21.9 folgt daraus mit $f=\chi$ die Absch. $|\Psi(y,\chi)|\ll U+\log(x)\,T_1(\chi)+T_2(\chi)+T_3(\chi)$

mit $T_1(\chi)=\sum_{\ell\leq\max(U,V)}\max_{w}\left|\sum_{w<k\leq y/\ell}\chi(k\ell)\right|$, $T_i(\chi)=\left|\sum_{U<m\leq\max(U,V,\frac{x}{V})}\ \sum_{k\leq\frac{x}{m}} a_i(m)b_i(k)\chi(mk)\right|$, $i=2,3$.

Dabei werden U,V nur von x und Q abh. gewählt, so dass

$$\sum_{q\leq Q}\frac{q}{\varphi(q)}\sum_{\chi(q)}^{*}|\Psi(y(\chi),\chi)|\ll UQ^2+\log(x)K_1+K_2+K_3,\quad K_j:=\sum_{q\leq Q}\frac{q}{\varphi(q)}\sum_{\chi(q)}^{*}T_j(\chi).$$

Haben für $q>1$, dass $\sum_{w<k\leq z}\chi(k)\ll\sqrt{q}\log(q)$ laut Polya–Vinogradov (Ü B/.8 A1(b)), für K_1 (wird $q=1$ triv. abgesch.) folgt

$$K_1\ll\max(U,V)\sum_{2\leq q\leq Q}q^{3/2}\log(q)+\sum_{\ell\leq\max(U,V)}\frac{x}{\ell}\ll\left(Q^{5/2}\max(U,V)+x\right)\log(x).$$

Für K_2, K_3 betr. $M \le x$, und für zth. Fktn. a, b betr. den Ausdruck

$$K_M := \sum_{q\le Q} \frac{q}{\varphi(q)} \sum_{\chi(q)}{}^{*} \Big| \underbrace{\sum_{M<m\le 2M} \sum_{k\le x/m}}_{\to\, k\le \frac{x}{M},\ km\le x} a(m) b(k) \chi(mk) \Big| \underset{\text{Satz } 21.4}{\ll} \log(x)(Q^2+M)^{\frac12}(Q^2+N)^{\frac12} \Big(\underbrace{\sum_{M<m\le 2M} |a(m)|^2}_{\ll M\log^2(M)}\Big)^{\frac12} \Big(\underbrace{\sum_{k\le x/M} |b(k)|^2}_{\ll \frac{x}{M}\log^3(\frac{x}{M})}\Big)^{\frac12}$$

$\forall a: |a(m)| \le \log(m)$ $\qquad$ $\forall b: |b(k)| \le \sum_{\le k} 1$

Es folgt $K_M \ll \log^4(x)\cdot\left(Q^2\sqrt{x} + Qx M^{-\frac12} + Q(xM)^{\frac12} + x\right)$.

Sei $W := \max(UV, \frac{x}{V}) \le x$. Für $M = 2^\nu U$, $\nu = 0,1,2,\dots$ und $M \le W$ summiere auf, mit $\nu \ll \log(x)$ folgt

$$\sum_{q\le Q} \frac{q}{\varphi(q)} \sum_{\chi(q)}{}^{*} \Big| \sum_{U<m\le W} \sum_{k\le x/m} a(m) b(k) \chi(mk) \Big|$$

$$\ll \log^5(x)\left(Q^2\sqrt{x} + Qx U^{-\frac12} + Q(xW)^{\frac12} + x\right),$$

mit $a = a_j$, $b = b_j$ für $j = 2,3$ entstehen die Summen K_j, es folgt

$$K_2 + K_3 \ll \log^5(x)\cdot\left(Q^2\sqrt{x} + Qx U^{-\frac12} + Qx V^{-\frac12} + Q(xUV)^{\frac12} + x\right).$$

• Nun setze $U = V$, $U := \begin{cases} x^{2/3}Q^{-1}, & x^{1/3} \le Q \le x^{1/2}, \quad \ulcorner \rightsquigarrow \frac{Qx}{U^{1/2}} \ll \sqrt{x}\,Q^2,\ x^{\frac12}\cdot x^{\frac23} \ll Qx^{\frac56} \lrcorner \\ x^{1/3}, & Q < x^{1/3}. \quad \ulcorner \to \frac{x}{U^{1/2}} = x^{5/6},\ Q^{5/2}x^{\frac13} \ll Q^2\sqrt{x} \lrcorner \end{cases}$

Es folgt die Beh. □

21.15. <u>Beweis des Satzes von B-V:</u> Schreibe $\Psi'(x,\chi) := \begin{cases} \Psi(x,\chi), & \chi \ne \chi_0, \\ \Psi(x,\chi_0) - x, & \chi = \chi_0. \end{cases}$

Dann ist $E(y;q,a) = \Psi(x,q,a) - \frac{y}{\varphi(q)} = \frac{1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a)\Psi'(y,\chi)$,

also

$$\max_{(a,q)=1} |E(y;q,a)| \le \frac{1}{\varphi(q)} \sum_{\chi(q)} |\Psi'(y,\chi)|.$$

Wird $\chi(q)$ von dem primitiven Charakter χ_1 mod q_1 induziert (wo $q_1 | q$), gilt $\Psi'(y,\chi) - \Psi'(y,\chi_1) \ll \log^2(qy)$, also $\max_{(a,q)=1} |E(y;q,a)| \ll \frac{1}{\varphi(q)} \sum_{\chi(q)} |\Psi'(y,\chi_1)| + \log^2(qy)$.

Das Bilden von $\max_{y\le x}$ und $\sum_{q\le Q}$ darüber liefert

$$\text{l.S.} := \sum_{q\le Q} \max_{y\le x} \max_{(a,q)=1} |E(y;q,a)| \ll \sum_{q\le Q} \frac{1}{\varphi(q)} \sum_{\chi(q)} \max_{y\le x} |\Psi'(y,\chi_1)| + Q\log^2(Qx).$$

Terme mit demselben χ_1 fassen wir zusammen: Da jeder primitive Charakter χ_1 mod q_1 genau einen Charakter χ zu jedem q mit $q_1 | q$ induziert, folgt

$$\text{l.S.} \ll \sum_{q_1 \le Q} \sum_{\chi_1(q_1)}^{*} \sum_{\ell \le \frac{Q}{q_1}} \frac{1}{\varphi(q_1 \ell)} \max_{y \le x} |\Psi'(y,\chi_1)| + Q \log^2(Qx).$$

Schreibe χ für χ_1 und q für q_1, wegen $\varphi(q\ell) \ge \varphi(q)\varphi(\ell)$ folgt

$$\text{l.S.} \ll \log(Q) \sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{\chi(q)}^{*} \max_{y \le x} |\Psi'(y,\chi_1)| + Q \log^2(Qx).$$

spalte auf in $q \le Q_1$ ($\rightsquigarrow$ S.-W.!) und $Q_1 < q \le Q$, wähle $Q_1 := \log^{A+6}(x)$.

Eine p.Σ mit Vaughans Lemma 21.14 liefert $\sum_{Q_1 < q \le Q} \frac{1}{\varphi(q)} \sum_{\chi(q)}^{*} \max_{y \le x} |\Psi'(y,\chi)| \ll \left(\frac{x}{Q_1} + x^{\frac{5}{6}} \log(Q) + x^{\frac{1}{2}} Q\right) \log^5(Qx)$.

- Ist nun $q > Q_1$ und $\chi(q)$ primitiv, ist $\Psi(y,\chi) = \Psi'(y,\chi)$, so dass damit im Bereich $Q_1 < q \le Q$ die behauptete Absch. gefunden ist.
- Ist $q \le Q_1$, gilt $\Psi'(y,\chi) \ll_A \frac{x}{\log^{2A}(x)}$ nach dem Satz von Siegel-Walfisz, die l.S. dann $\ll \frac{x}{\log^A(x)}$. Es folgt die Beh. □

21.16. Bem.: • Der Bereich $Q \ll \frac{x^{1/2}}{\log(x)}$ im Satz von B-V ist wesentlich.

- Laut Elliott-Halberstam-Vermutung (EH) müsste für $Q \ll x^{1-\varepsilon}$, $\varepsilon > 0$ bel., die Abschätzung im Satz von B-V gelten. Diese Vermutung ist neuerdings im Zusammenhang mit dem kleinen PZ-Lückenproblem zentral geworden, vgl. a20.19.
- Gilt die Absch. für $Q \ll x^{\delta - \varepsilon}$, $\varepsilon > 0$ bel., so wird $\delta > 0$ auch als Level of distribution bezeichnet. Laut B-V haben wir $\delta = \frac{1}{2}$, laut (EH) gilt vermutlich $\delta = 1$.
- Zahlreiche Varianten des Satzes wurden bis heute veröffentlicht. Speziell diejenigen, bei denen die Moduln q von spezieller Form sind, z.B. Polynomwerte, glatt, usw. Gelegentlich können solche Varianten den von B-V vorgegebenen level of distribution übersteigen und gewinnbringend in dafür zugeschnittenen Anwendungen eingesetzt werden.
- Der Satz von B-V hat zahlreiche Anwendungen in der zth. Literatur. Bombieri wurde (vor allem für diesen Satz) im Jahr 1974 mit der Fields-Medaille ausgezeichnet.

Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a22: Kreismethode und Goldbachproblem

Stichworte: Goldbachsche Vermutung, Waring-Problem, Heuristik Kreismethode, major und minor arcs im ternären Goldbach Problem, Satz von Vinogradov, singuläre Reihe

---

22.1. Einleitung:

Additive Zahlentheorie-Probleme: Für Teilmengen $\mathcal{A}_1, \dots, \mathcal{A}_k \subseteq \mathbb{N}$ sei die Summenmenge $\mathcal{A}_1 + \dots + \mathcal{A}_k := \{ n \in \mathbb{N} ; \exists\, a_i \in \mathcal{A}_i, 1 \le i \le k : n = a_1 + \dots + a_k \}$.

- Von einem direkten additiven Problem spricht man, wenn man etwa $\mathcal{A} = \mathcal{A}_1 + \dots + \mathcal{A}_k$ beweisen möchte für eine bestimmte feste Teilmenge $\mathcal{A} \subseteq \mathbb{N}$.
- Von einem inversen additiven Problem spricht man, wenn man aus $\#\mathcal{A}$ und anderen Eigenschaften von $\mathcal{A}$ auf $\mathcal{A}_i$ mit $\mathcal{A} = \mathcal{A}_1 + \dots + \mathcal{A}_k$ schließen möchte.

Wir möchten in diesem Kapitel nur direkte additive Probleme besprechen. Darunter fällt insb. die Goldbach-Vermutung und das Waring-Problem.

22.2. Die Goldbach-Vermutung: Aus dem Briefwechsel von 1742 zwischen Euler und Goldbach:

(1) $n \in \mathbb{N}_{>1} \Rightarrow \exists\, p_1, p_2 \in \mathbb{P} : 2n = p_1 + p_2$? (binäres Problem, ungelöst)

(2) $n \in \mathbb{N}_{>2} \Rightarrow \exists\, p_1, p_2, p_3 \in \mathbb{P} : 2n + 1 = p_1 + p_2 + p_3$? (ternäres Problem, gelöst von [Vinogradov 1937] für alle $n > n_0$, arXiv-Beweis: [H. Helfgott, 2013].

Das Waring-Problem: E. Waring behauptete 1770 ohne Beweisangabe, dass jede nat. Zahl die Summe von 4 Quadraten, 9 Kuben, 19 4-ten Potenzen usw. sei.

Formal: $\forall k \ge 2\ \exists\, g(k) \in \mathbb{N}\ \forall n \in \mathbb{N} : \exists\, a_1, \dots, a_\ell \in \mathbb{N} : n = a_1^k + \dots + a_\ell^k,\ 1 \le \ell \le g(k)$.

- Für $k = 2$ liefert der Satz von Lagrange den Wert $g(2) = 4$.
- [Wieferich & Kempner 1910]: $g(3) = 9$, was optimal ist, da 23, 239 nicht als Summe von ≤ 8 Kuben geschrieben werden können.
- [Hilbert 1909]: $g(k) < \infty$ bewiesen

• Um 1919 entwickelten Hardy/Littlewood/Ramanujan die Kreismethode, die zunächst zur Lösung des Waring-Problems diente, aber tatsächlich auch das Goldbach-Problem und allgemeiner bel. direkte additive Probleme behandeln kann und bis heute verwendet wird.

Beispielsweise wird die quantitative Version der PZ-Zwillings-Vermutung in 17.9 mit der Kreismethode ermittelt. Das ternäre Goldbachproblem haben Hardy & Littlewood so bereits unter Ann. der (GRH) für alle $n \geq n_0$ (zur Behandlung der minor arcs) gelöst.

22.3. Heuristik Kreismethode: Betr. die Anzahl Darstellungen, n als Summe von El. aus $\mathcal{A}_1, \dots, \mathcal{A}_k$ zu schreiben:

$$R(n) := \sum_{\substack{a_i \in \mathcal{A}_i \\ n = a_1 + \dots + a_k}} 1 = \#\{(a_1, \dots, a_k) \in \mathcal{A}_1 \times \dots \times \mathcal{A}_k;\ n = a_1 + \dots + a_k\}.$$

Ziel: z.z. $R(n) \overset{!}{>} 0$ oder $R(n) \overset{!}{\gg} 1$ oder noch besser, wenigstens für alle hinr. großen $n \geq n_0$ oder ∞ viele n.

Die Grundidee ist, eine Fourieranalyse durchzuführen: man gehe über zur komplexen Exponentialsumme $T_i(\alpha) = \sum_{\substack{m \in \mathcal{A}_i \\ m \leq x}} e(\alpha m)$, wo $e(\alpha) = e^{2\pi i \alpha}$, $x \geq n$ oder $x = n$, dann schreibe $R(n)$ als komplexes $\int$, denn $R(n) = \int_0^1 T_1(\alpha) \cdots T_k(\alpha)\, e(-n\alpha)\, d\alpha$.

$$\text{r.S.} = \sum_{m_i \in \mathcal{A}_i} \underbrace{\int_0^1 e(\alpha(m_1 + m_2 + \dots + m_k - n))\, d\alpha}_{\overset{\text{Orthogonalitätsrelation}}{=} \begin{cases} 1, & m_1 + m_2 + \dots + m_k - n = 0, \\ 0, & \text{sonst} \end{cases}} = R(n). \quad \text{J}$$

Vgl. Ü Blatt 5 A3(a)

Die Kreismethode beruht nun auf der Beobachtung, dass der Wert des $\int_0^1$ vor allem durch den Wert auf bestimmten Teilintervallen von $[0,1]$ gegeben ist. Man nennt diese maßgeblichen Teilintervalle die "major arcs" und die Restintervalle die "minor arcs" (ursprünglich "arc" als Bogen (wegen $e(\alpha) = e^{2\pi i \alpha}$ auf Einheitskreis $|z| = 1$) interpretiert). Die genaue Wahl dieser arcs hängt aber vom konkreten Problem ab.

22.4. <u>Mehr quantitative Heuristik:</u>

Betr. nun mit $T_1(\alpha)\cdots T_n(\alpha) =: T(\alpha)$ eine einzige Exponentialsumme $T(\alpha) = \sum_{m\le x} c_m e(\alpha m)$.

Dann ist $c_N = \int_0^1 T(\alpha) e(-N\alpha)\,d\alpha \underset{\text{Riemann}\Sigma}{=} \lim_{q\to\infty} \frac{1}{q}\sum_{a\le q} T(\frac{a}{q}) e(-N\frac{a}{q})$. ⊛.

- Integrand bei $\alpha = \frac{a}{q} \in \mathbb{Q}$: $T(\frac{a}{q}) e(-N\frac{a}{q}) = \sum_m c_m e(\frac{a}{q}(m-N))$

$$= \sum_{m\equiv N(q)} c_m \cdot 1 + \sum_{m\equiv N+1(q)} c_m e(\tfrac{a}{q}) + \sum_{m\equiv N+2(q)} c_m e(2\tfrac{a}{q}) + \dots + \sum_{m\equiv N+q-1(q)} c_m e((q-1)\tfrac{a}{q})$$

alle q-ten Einheitswurzeln

Als Bsp., im einfachen Fall, wenn alle $c_m = 1$, sind alle $\sum_{m\equiv N+j(q)} c_m \approx \frac{x}{q}$ etwa gleich, und stellen "Ausschläge" bzw. "Peaks" des Integranden dar.
(Im Prinzip könnten sich diese aber auch wieder wegheben.)

- Integrand nahe $\frac{a}{q}$, d.h. bei $\alpha = \frac{a}{q} + \beta$ mit $|\beta| > 0$ klein:

$$T(\tfrac{a}{q}+\beta) e(-N(\tfrac{a}{q}+\beta)) = \sum_m c_m e(\tfrac{a}{q}(m-N)) \cdot \underbrace{e(\beta(m-N))}_{\approx 1 \text{ für } \beta\approx 0}$$ ← "Peaks" ungefähr wie bei a/q

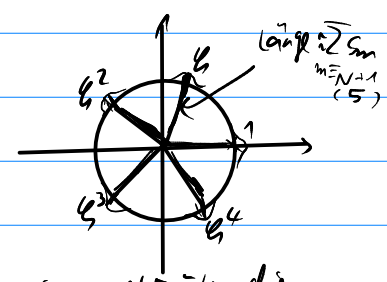
22.5. <u>Bsp.:</u> $\frac{a}{q} = \frac{1}{5}$: $T(\frac{1}{5}) e(-N\cdot\frac{1}{5}) = \sum_{m\equiv N(5)} c_m + \sum_{m\equiv N+1(5)} c_m \zeta + \dots + \sum_{m\equiv N+4(5)} c_m \zeta^4$

$\zeta = e(\frac{1}{5})$ die 5-te EW

Wir erhalten Frequenzbilder $f(\beta) = T(\frac{a}{q}+\beta) e(-N(\frac{a}{q}+\beta))$ für β klein, d.h. Ausschläge nahe $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ als "Zerlegung in Frequenzen":

Die Summe der Ausschläge bzw. Überlagerung liefert in etwa den Wert von $T(\alpha) e(-N\alpha)$.

⌈Aus ⊛ folgt: $\underbrace{\frac{1}{Q}\sum_{q\le Q}}_{\text{Mittelwert von ⊛}} \underbrace{\frac{1}{q}\sum_{a\le q} T(\frac{a}{q}) e(-N\frac{a}{q})}_{\text{Überlagerungen für alle } q\le Q,\ a\le q} \xrightarrow{Q\to\infty} c_N$. ⌋



(summiert über diese Vektoren)

↳ zusammen mit Überlagerung der Bilder bei $q=2$, $q=3$, $q=4$, ...

22.6. **Kreismethode im ternären Goldbach-Problem:**
Für $\alpha \in \mathbb{R}$ sei $S(\alpha) := \sum_{p \le n} \log(p)\, e(\alpha p)$ und $R(n) := \sum_{p_1+p_2+p_3=n} \log(p_1)\log(p_2)\log(p_3)$.

Die zusätzliche Gewichtung mit $\log(p)$ macht die Behandlung der PZsummen technisch einfacher; vergleichbar mit $\pi \to \vartheta$ beim PZS. Haben: $R(n) = \int_0^1 S^3(\alpha) e(-n\alpha)\, d\alpha$.

- Wahl der major arcs $\mathfrak{M} \subseteq [0,1]$: Sei $B > 0$, $Q := \log^B(n)$. Für $1 \le q \le Q$, $0 \le a \le q$ mit $(a,q) = 1$ def. den major arc $\mathfrak{M}(a,q) := [\frac{a}{q} - \frac{Q}{n}, \frac{a}{q} + \frac{Q}{n}] \cap [0,1]$.
und $\mathfrak{M} := \bigcup_{q \le Q} \bigcup_{\substack{0 \le a \le q \\ (a,q)=1}} \mathfrak{M}(a,q) \subseteq [0,1]$.

Bel.: Die major arcs sind p.w. disjunkt für große n. $\ulcorner \alpha \in \mathfrak{M}(a,q) \cap \mathfrak{M}(a',q')$, wo $\frac{a}{q} \ne \frac{a'}{q'}$
$\Rightarrow \frac{1}{Q^2} \le \frac{1}{qq'} \le \frac{|aq'-a'q|}{qq'} = |\frac{a}{q} - \frac{a'}{q'}| \le |\frac{a}{q} - \alpha| + |\alpha - \frac{a'}{q'}| \le 2\frac{Q}{n} \Rightarrow n \le 2Q^3 = 2(\log(n))^{3B}$,
was für alle hinr. großen n nicht stimmt.)

- Wahl der minor arcs als $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.
- Aufspaltung: $R(n) = \int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} S^3(\alpha) e(-n\alpha)\, d\alpha$.

$\rightsquigarrow$ ergibt Asymptotik, erwarten Hauptterm in $\int_{\mathfrak{M}}$, $\int_{\mathfrak{m}}$ trägt zum Fehlerterm bei (obwohl Maß von $\mathfrak{M}$ gegen 0 geht bei $n \to \infty$)

22.7. **Major arcs im ternären Goldbachproblem:** Hier (wie meist) ist die Auswertung von $\int_{\mathfrak{M}}$ eine direkte Rechnung. Im wesentlichen muss $S(\frac{a}{q})$ berechnet werden:

$$S(\tfrac{a}{q}) = \sum_{\substack{r \le q \\ (r,q)=1}} \sum_{\substack{p \le n \\ p \equiv r (q)}} \log(p)\, \underbrace{e(\tfrac{a}{q}p)}_{= e(\frac{a}{q}r)} + \underbrace{O(\log(q))}_{\text{für die } r \text{ mit } (r,q)>1} = \sum_{\substack{r \le q \\ (r,q)=1}} e(\tfrac{ar}{q}) \cdot \sum_{\substack{p \le n \\ p \equiv r (q)}} \log(p) + O(\log(q))$$

Für die PZsumme wird jetzt der Satz von Siegel-Walfisz 11.6 eingesetzt. Nach diesem ist die PZsumme $\approx \frac{n}{\varphi(q)}$.
Die zahlentheoretische Funktion $c_q(a) := \sum_{\substack{r \le q \\ (r,q)=1}} e(\frac{ar}{q})$ heißt Ramanujan-Summe.
Für sie ist $c_q(a) = \mu(q)$ für $(a,q)=1$

Also ist $S(\frac{a}{q}) = \frac{\mu(q)}{\varphi(q)} n + \text{Fehlerterm}$.

Um $S(\frac{a}{q}+\beta)$ auszuwerten, ist jetzt noch eine partielle Summation erforderlich; sie zeigt, dass $S(\frac{a}{q}+\beta) = \frac{\mu(q)}{\varphi(q)} \sum_{m\le n} e(\beta m)$ + Fehlerterm ist.

Insg. folgt so:

Satz: Für $A>0$ ex. $B(A)>0$, so dass für $Q := \log^B n$ (in der Def. von $\mathfrak{M}$) gilt:

$$\int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha)\, d\alpha = \mathfrak{S}(n)\cdot\frac{n^2}{2} + O\left(\frac{n^2}{\log^A n}\right),$$

wobei die O-Konstante nur von A abhängt. Dabei heißt $\mathfrak{S}(n) := \sum_{q=1}^{\infty} \frac{\mu(q)\, c_q(-n)}{\varphi(q)^3}$ die singuläre Reihe des ternären Goldbachproblems. ← absolut kgt.! $\left[|c_q(-n)| \le \varphi(q)\right]$

22.8. **Minor arcs im ternären Goldbachproblem**: Sei nun $\alpha \in \mathfrak{m}$. Nach dem Dirichletschen Approximationssatz 222.8 (ZTI) gibt es einen Bruch $\frac{a}{q}$, $(a,q)=1$, mit $q \le \frac{n}{Q}$ und $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q\cdot\frac{n}{Q}} = \frac{Q}{nq} \left(\le \frac{1}{q^2}\right)$. Da $\alpha \in \mathfrak{m}$, gilt für dieses q dann $q > Q = \log^B(n)$, denn sonst wäre ja $\alpha \in \mathfrak{M}(a,q) \subseteq \mathfrak{M}$ ↯.

Demnach sind die Punkte α der minor arcs nur mit gekürzten Brüchen von großem Nenner q approximierbar. Ist q groß, kann mit folgendem Satz eine nichttriviale obere Schranke für $|S(\alpha)|$ gezeigt werden; dies zeigt, dass $\int_{\mathfrak{m}}$ ein Fehlerterm ist.

22.9. **Satz von (Vinogradov/Vaughan)**: Gilt $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}$, $1 \le q \le n$, $(a,q)=1$, so ist

$$S(\alpha) \ll \left(\frac{n}{q^{1/2}} + n^{4/5} + n^{1/2} q^{1/2}\right)(\log(n))^4.$$

[Beweis: z.B. [Nathanson, Lemma 8.8]; benutzt + (im Prinzip) Vaughans Identität 21.7.]

Mit diesem Satz kann die (GRH) aus dem Beweis von Hardy & Littlewood eliminiert werden.

Zusammenfassung des Ergebnisses:

22.10. **Satz von Vinogradov**: Es gibt eine zahlentheoretische Fkt. $\mathfrak{S}(n)$ und $c_1, c_2 > 0$ mit $c_1 < \mathfrak{S}(n) < c_2$ für alle ungeraden n, so dass für alle $n \ge n_0$ gilt:

$$R(n) = \mathfrak{S}(n)\frac{n^2}{2} + O\left(\frac{n^2}{\log^A n}\right).$$

[Für $r(n) = \sum_{p_1+p_2+p_3=n} 1$ kann mit partieller Σ daraus $r(n) = \mathfrak{S}(n)\frac{n^2}{2\log^2 n}\left(1 + O\left(\frac{\log\log n}{\log n}\right)\right)$ hergeleitet werden.]

Damit ist für alle ungeraden $n \ge n_0$ also $R(n) > 0$ gezeigt [weil dann Fehlerterm < Hauptterm].

Dazu bleibt noch die (untere) Abschätzung von $\mathfrak{S}(n)$ zu zeigen.

22.11. **Satz (Eulerproduktdarstellung der singulären Reihe):** Es gilt

$$\mathfrak{S}(n) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

Insb. ist also $\mathfrak{S}(n)=0$ für gerade n und $1 \ll \mathfrak{S}(n) \ll 1$ für ungerade n.

Bew.: Die zahlentheoretische Fkt. $\frac{\mu(q)c_q(-n)}{\varphi(q)^3}$ ist multiplikativ in q, da $c_q(-n)$ multiplikativ in q ist. Der Euler-Produktsatz liefert also

$$\mathfrak{S}(n) = \prod_p\Big(1+\underbrace{\sum_{k=1}^{\infty}\frac{\mu(p^k)c_{p^k}(-n)}{\varphi(p^k)^3}}_{=0 \text{ für } k\geq 2}\Big) = \prod_p\left(1-\frac{c_p(-n)}{\varphi(p)^3}\right) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

$$c_p(-n) = \begin{cases} p-1, & p\mid n \\ -1, & \text{sonst}\end{cases}$$

$\square$

22.12. **Bem.:** Die singuläre Reihe ist $=0$ für gerade n. Wäre dies nicht so, würde der Satz 22.10 von Vinogradov bereits das binäre Goldbachproblem positiv entscheiden; für $n>6$ gerade ist in $n=p_1+p_2+p_3$ notwendig ein $p_i=2$, etwa $p_1=2$ und (jedes) $n-p_1=p_2+p_3$ wäre Summe zweier PZen. Stattdessen zeigt 22.10 nur eine obere Absch. für $R(n)$ in diesem Fall, so dass die Methode dann "zusammenbricht" bzw. ein "singulärer Fall" vorliegt; daher der Begriff "singuläre Reihe".

ENDE der Vorlesung ZT II