3.4 Die erweiterte Riemannsche Vermutung (ERH)

Ein **Charakter** mod n ist eine Funktion

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

mit den Eigenschaften:

(i) χ hat die Periode n.

(ii) $\chi(xy) = \chi(x)\chi(y)$ für alle $x, y \in \mathbb{Z}$.

(iii) $\chi(x) = 0$ genau dann, wenn $\mathrm{ggT}(x, n) > 1$.

Die Charaktere mod n entsprechen kanonisch bijektiv genau den Gruppen-Homomorphismen

$$\bar{\chi} : \mathbb{M}_n \longrightarrow \mathbb{C}^\times.$$

Beispiele sind der **triviale Charakter** $\chi(a) = 1$ für alle zu n teilerfremden a und der aus der Theorie der quadratischen Reziprozität bekannte Jacobi-**Charakter** $\chi(a) = (\frac{a}{n})$, siehe Anhang A.5.

Zu einem Charakter gehört eine **L-Funktion**, die durch die Dirichlet-Reihe

$$L_\chi(z) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^z}$$

definiert ist. Die Reihe konvergiert absolut und lokal gleichmäßig in der Halbebene $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 1\}$, weil $a^{i\cdot \mathrm{Im}(z)} = e^{i\cdot \ln(a)\cdot \mathrm{Im}(z)}$ den Betrag 1 hat, also

$$\left|\frac{\chi(a)}{a^z}\right| = \left|\frac{\chi(a)}{a^{\mathrm{Re}(z)} \cdot a^{i\cdot \mathrm{Im}(z)}}\right| = \frac{1}{a^{\mathrm{Re}(z)}} \qquad \text{oder } 0.$$

Sie läßt sich analytisch auf die rechte Halbebene $\mathrm{Re}(z) > 0$ fortsetzen und ist dort holomorph, außer im Fall des trivialen Charakters, wo 1 ein einfacher Pol ist. Die Funktion L_χ hat die Riemann-**Eigenschaft**, wenn sie innerhalb des Streifens $0 < \mathrm{Re}(z) \leq 1$ Nullstellen nur auf der Geraden $\mathrm{Re}(z) = \frac{1}{2}$ hat. Die Riemannsche Vermutung behauptet dies gerade für die Riemannsche Zeta-Funktion, die **erweiterte** Riemannsche **Vermutung** für alle L-Funktionen zu Charakteren mod n. Die Zeta-Funktion ist für $\mathrm{Re}(z) > 1$ definiert durch

$$\zeta(z) := \sum_{a=1}^{\infty} \frac{1}{a^z} = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^z}},$$

wobei die zweite Gleichung die Produktformel von Euler ist. Für den trivialen Charakter χ_1 mod n gilt also:

$$L_{\chi_1}(z) = \sum_{\mathrm{ggT}(a,n)=1} \frac{1}{a^z} = \zeta(z) \cdot \prod_{p|n \text{ prim}} \left(1 - \frac{1}{p^z}\right);$$

diese L-Funktion hat in $\mathrm{Re}(z) > 0$ die gleichen Nullstellen wie ζ.

Satz 3 (ANKENEY/MONTGOMERY/BACH) *Für $c = 2/\ln(3)^2 = 1.65707\ldots$ gilt: Ist χ ein nichttrivialer Charakter* mod n*, dessen L-Funktion L_χ die* RIEMANN*-Eigenschaft hat, so gibt es eine Primzahl $p < c \cdot \ln(n)^2$ mit $\chi(p) \neq 1$.*

Der Beweis soll hier nicht geführt werden.

Korollar 1 *Es gelte die verallgemeinerte* RIEMANN*sche Vermutung. Sei $G < \mathbb{M}_n$ eine echte Untergruppe. Dann gibt es eine Primzahl p mit $p < c \cdot \ln(n)^2$, deren Restklasse* mod n *im Komplement $\mathbb{M}_n - G$ liegt.*

Beweis. Es gibt einen nichttrivialen Homomorphismus $\mathbb{M}_n/G \longrightarrow \mathbb{C}^\times$, also einen Charakter mod n mit $G \subseteq \operatorname{Kern}\chi \subseteq \mathbb{M}_n$. $\diamond$

Satz 4 (MILLER) *Die ungerade Zahl $n \geq 3$ bestehe den strengen Pseudoprimzahltest für alle primen Basen $a < c \cdot \ln(n)^2$ mit c wie in Satz 3, und die L-Funktion jedes Charakters für jeden Teiler von n habe die Riemann-Eigenschaft. Dann ist n prim.*

Beweis. Zuerst wird gezeigt, dass n quadratfrei ist. Angenommen $p^2 \mid n$ für eine Primzahl p. Die multiplikative Gruppe $\mathbb{M}_{p^2}$ ist zyklisch von der Ordnung $p(p-1)$; insbesondere ist der Homomorphismus

$$\mathbb{M}_{p^2} \longrightarrow \mathbb{M}_{p^2}, a \mapsto a^{p-1} \bmod p^2,$$

nichttrivial. Sein Bild ist eine Untergruppe $G < \mathbb{M}_{p^2}$ der Ordnung p, die zyklisch, also isomorph zur Gruppe der p-ten Einheitswurzeln in $\mathbb{C}$ ist. Die Zusammensetzung ergibt einen Charakter mod p^2, und Satz 3 ergibt eine Primzahl $a < c \cdot \ln(p^2)^2$ mit $a^{p-1} \not\equiv 1 \bmod p^2$. Die Ordnung von a in $\mathbb{M}_{p^2}$ teilt $p(p-1)$. Wäre $a^{n-1} \equiv 1 \bmod n$, so müsste die Ordnung auch $n-1$ teilen. Da p zu $n-1$ teilerfremd ist, müsste sie Teiler von $p-1$ sein, was sie ja gerade nicht ist. Also ist $a^{n-1} \not\equiv 1 \bmod n$, und das widerspricht nun wieder dem bestandenen Pseudoprimzahltest. Also ist n quadratfrei.

Jetzt wird gezeigt, dass n auch nicht zwei verschiedene Primfaktoren haben kann. Nehmen wir an, p und q seien zwei solche, o. B. d. A. $\nu_2(p-1) \geq \nu_2(q-1)$. [$\nu_2(x)$ der Exponent des Primfaktors 2 in x.] Sei

$$r = \begin{cases} p, & \text{falls } \nu_2(p-1) > \nu_2(q-1), \\ pq, & \text{falls } \nu_2(p-1) = \nu_2(q-1). \end{cases}$$

Wieder nach dem Satz 3 gibt es ein $a < c \cdot \ln(r)^2$ mit $(\frac{a}{r}) = -1$. Ist u der ungerade Teil von $n-1$ und $b = a^u$, so ist auch $(\frac{b}{r}) = -1$, insbesondere $b \neq 1$. Wegen des strengen Pseudoprimzahltests gibt es also ein k mit $b^{2^k} \equiv -1 \bmod n$. Dann hat also b in $\mathbb{M}_p$ und in $\mathbb{M}_q$ die Ordnung 2^{k+1}. Insbesondere ist $2^{k+1} \mid q-1$.

Falls nun $\nu_2(p-1) > \nu_2(q-1)$ ist, muss sogar $2^{k+1} \mid \frac{p-1}{2}$ sein. Daraus folgt im Widerspruch zum EULER-Kriterium $b^{(p-1)/2} \equiv 1 \pmod{p}$, aber $(\frac{b}{p}) = -1$.

Ist aber $\nu_2(p-1) = \nu_2(q-1)$, so $(\frac{b}{p})(\frac{b}{q}) = (\frac{b}{r}) = -1$; also o. B. d. A. $(\frac{b}{p}) = -1$, $(\frac{b}{q}) = 1$. Nach dem EULER-Kriterium ist $b^{(q-1)/2} \equiv 1 \pmod{q}$, also $2^{k+1} \mid \frac{q-1}{2}$, $k+2 \leq \nu_2(q-1) = \nu_2(p-1)$, also auch $b^{(p-1)/2} \equiv 1 \pmod{p}$, im Widerspruch zu $(\frac{b}{p}) = -1$. $\diamond$

Für den Primzahltest von Miller reicht es also, den strengen Pseudoprimzahltest für alle Primzahlen $a < c \cdot \ln(n)^2$ durchzuführen. Der Gesamtaufwand ist also $O(\log(n)^5)$. Für eine 512-Bit-Zahl, also $n < 2^{512}$, reicht es, die 18698 Primzahlen < 208704 durchzuprobieren. Das dauert natürlich bei aller Effizienz seine Zeit. In der Praxis hat sich daher eine Modifikation dieses Tests durchgesetzt, die (in einem noch zu spezifizierenden Sinne) nicht ganz exakt, aber wesentlich schneller ist. Sie wird im nächsten Abschnitt behandelt.