Technische Universität Clausthal
Institut für Mathematik
Prof. Dr. L. G. Lucht

WS 1999/2000
31.01.2000
12. Übungsblatt

Elementare Zahlentheorie

Diese Aufgaben werden in der Übungsstunde vom 09.02.2000 besprochen;
Abgabe schriftlicher Lösungen bitte am Montag, 07.02.2000, vor der Vorlesung.

1. (a) Es sei p eine ungerade Primzahl. Zeigen Sie, daß das Legendre-Symbol $\left(\frac{\bullet}{p}\right)$ ein reeller Charakter modulo p ist.

   (b) Es seien $p_1, \ldots, p_r$ verschiedene ungerade Primzahlen. Wieviele reelle Charaktere gibt es modulo $q = p_1 \cdots p_r$? (Mit genauer Begründung!)

   Geben Sie die Anzahl der reellen Charaktere für beliebiges $q \in \mathbb{N}$ an. (Kurze Begründung genügt!)

2. Zeigen Sie $1 < (s-1)\,\zeta(s) < s$ für $s > 1$ und folgern Sie $\lim\limits_{s \to 1+} (s-1)\,\zeta(s) = 1$.

3. (a) Beweisen Sie Lemma 2 der Vorlesung: Es sei $\operatorname{ggT}(a, q) = 1$, und a habe in $G(q)$ die Ordnung h, so daß $\chi(a)$ eine h-te Einheitswurzel ist. Alle h-ten Einheitswurzeln werden von $\chi(a)$ gleichhäufig angenommen, wenn χ alle Restklassencharaktere modulo q durchläuft (Hinweis: Vergleichen Sie dies mit dem Beweis, daß Nebenklassen von Untergruppen gleichgroß sind).

   (b) Erläutern Sie damit folgende Rechnung: Es sei $\xi = \exp\left(\frac{2\pi i}{h}\right)$, $z = p^{-s}$ und $p \nmid q$. Dann ist

$$\prod_{\chi \in \widehat{G}(q)} \left(1 - \chi(p)\,p^{-s}\right) = \prod_{\lambda=0}^{h-1} \left(1 - \xi^{\lambda} z\right)^{\frac{\varphi(q)}{h}} = \left(1 - z^{h}\right)^{\frac{\varphi(q)}{h}} = \left(1 - p^{-hs}\right)^{\frac{\varphi(q)}{h}} \leq 1\,.$$

4. Es sei χ ein reeller Charakter und $f = 1 * \chi$. Zeigen Sie

   (a) $f(n) \geq 0$ für $n \in \mathbb{N}$.

   (b) $f(m^2) \geq 1$ für $m \in \mathbb{N}$.

   (c) Folgern Sie, daß $\displaystyle\sum_{n=1}^{\infty} \frac{f(n)}{\sqrt{n}}$ divergiert.

5. (a) Beweisen Sie, daß es unendlich viele Primzahlen $p \equiv 1 \bmod 4$ gibt, indem Sie zeigen, daß die Primteiler der Funktionswerte des Polynoms $f(x) = 4x^2 + 1$ nur von der Form $p \equiv 1 \bmod 4$ sein können.

   (b) Beweisen Sie analog, daß es unendlich viele Primzahlen $p \equiv 1 \bmod 3$ gibt. Hinweis: Betrachten Sie die Primteiler von $f(x) = x^2 + x + 1$.

   (c) Versuchen Sie, (b) zu verallgemeinern: Zu jeder Primzahl q liegen in der Restklasse $1 \bmod q$ unendlich viele Primzahlen.