10. Übungsblatt

ZAHLENTHEORIE (SS 2007)

Abgabe: Mi. 20.6.2007, bis 9.10 Uhr

Fach Nr. 11 (orangener Schrank bei D1.348)

Internet: http://math-www.uni-paderborn.de/~chris

Schreiben Sie bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel–Nr. und Ihre Übungsgruppe. Heften Sie bitte die Seiten zusammen!

Die folgenden Aufgaben sind auf Grundlage der Vorlesung und der Übungen zu bearbeiten!

39. Aufgabe: a) Sei $n \in \mathbb{N}, n \geq 2$. Beweise die Äquivalenz der beiden folgenden Aussagen:

i) n ist eine Primzahl. **ii)** Es gilt $(n-1)! \equiv -1 \pmod{n}$.

b) Ist $p = 2n+1$ eine Primzahl, so gilt $(n!)^2 \equiv (-1)^{n+1} \pmod{p}$.

c) Leite aus b) her, daß im Falle einer Primzahl p mit $p \equiv 1 \pmod 4$ die Zahl -1 quadratischer Rest modulo p ist. (3)

40. Aufgabe: a) Sei $n \in \mathbb{N}$, $n \geq 3$ und sei w eine Primitivwurzel modulo n. Beweise für $k \in \mathbb{N}_0$: w^k QR mod $n \iff k$ gerade.

b) Beweise unter den Voraussetzungen von a), daß die Anzahl der QR'e modulo n mit der Anzahl der QNR'e modulo n übereinstimmt und gleich $\frac{1}{2}\varphi(n)$ ist.

c) Berechne die Anzahl der QR'e modulo 16 und die Anzahl der QNR'e modulo 16.

d) Sei $k \in \mathbb{N}$, $k \geq 3$. Bestimme die Anzahl der QR'e modulo 2^k und die Anzahl der QNR'e modulo 2^k. (5)

41. Aufgabe: p sei eine ungerade Primzahl. Die Zahlen $a, b \in \mathbb{Z}$ seien teilerfremd. Beweise:

a) $p \mid (a^2+b^2) \implies p \equiv 1 \pmod 4$.

b) $p \mid (a^4+b^4) \implies p \equiv 1 \pmod 8$. (3)

42. Aufgabe: (Fortsetzung von Aufgabe 29)

Sei p ein Primteiler der n–ten Fermat'schen Zahl F_n $(n \geq 2)$. Beweise:

a) Es gibt ein $k \in \mathbb{N}$ mit $p = k \cdot 2^{n+1} + 1$

b) Es gilt $p \equiv 1 \pmod 8$

c) $\mathrm{ord}_p(2)$ ist ein Teiler von $\frac{1}{2}(p-1)$

d) Es gibt ein $m \in \mathbb{N}$ mit $p = m \cdot 2^{n+2} + 1$. (3)

Wenn Sie mit dem **Korrektor** Andreas Kottmann sprechen wollen, schicken Sie ihm bitte eine email an die Adresse kottmann@zitmail.uni-paderborn.de