11. Übungsblatt

ZAHLENTHEORIE (SS 2007)

Abgabe: Mi. 27.6.2007, 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!

43. Aufgabe: Berechne die folgenden Legendre– bzw. Jacobi–Symbole:

a) $\left(\frac{5}{11}\right)$, $\left(\frac{7}{13}\right)$ mit Hilfe des Lemmas von Gauß (13.15) .

b) $\left(\frac{131}{151}\right)$, $\left(\frac{2340}{28041}\right)$, $\left(\frac{392}{667}\right)$. (3)

44. Aufgabe: a) p, p' und q seien ungerade Primzahlen. Beweise:

$$p \equiv p' \pmod{4q} \quad \Longrightarrow \quad \left(\frac{q}{p}\right) = \left(\frac{q}{p'}\right) .$$

b) Beweise: Zu jeder Primzahl $q > 5$ existiert eine Primzahl p mit $2 < p < q$ und $\left(\frac{q}{p}\right) = 1$. (3)

45. Aufgabe: $n > 2$ sei eine beliebige natürliche Zahl. Die Zahlen $a, b \in \mathbb{Z}$ seien beide teilerfremd zu n . Beweise:

a) Sind a und b QR'e modulo n , so ist auch $a \cdot b$ ein QR modulo n

b) Ist a ein QR modulo n und b ein QNR modulo n , so ist $a \cdot b$ ein QNR modulo n

c) Existiert eine PW modulo n , so ist das Produkt zweier QNR'e ein QR modulo n

d) Untersuche, ob die Aussage in c) für beliebige natürliche Zahlen > 2 richtig ist. (3)

46. Aufgabe: a) (Dieser Aufgabenteil ist unabhängig vom Teil b) zu bearbeiten!) Bestimme die Anzahl der Lösungen von $x^6 \equiv 1 \pmod{15}$. Wieviele 6–te Potenzreste modulo 15 gibt es? Was ist der Zusammenhang zwischen diesen beiden Anzahlen. Wieviele Lösungen hat die Kongruenz $x^6 \equiv 4 \pmod{15}$?

b) Seien $m, n \in \mathbb{N}$ mit $m \geq 2$. Es bezeichne k die Anzahl der modulo n verschiedenen Lösungen der Kongruenz $(\star)$ $x^m \equiv 1 \pmod{n}$. Beweise:

1) $E_m := \{\, [a]_n \mid a \text{ ist Lösung von } (\star) \,\}$ ist eine Untergruppe der Ordnung k von $\mathbb{Z}_n^\star$.

2) Ist $c \in \mathbb{Z}$ ein beliebiger m–ter Potenzrest modulo n , so hat die Kongruenz $x^m \equiv c \pmod{n}$ genau k verschiedene Lösungen modulo n

3) Es gibt genau $\frac{\varphi(n)}{k}$ verschiedene m–te Potenzreste modulo n . (5)

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