8. Übungsblatt

ZAHLENTHEORIE (SS 2007)

Abgabe: Mi. 6.6.2007, 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!

31. Aufgabe: w sei eine Primitivwurzel modulo n. Die Zahlen $a, b \in \mathbb{Z}$ seien beide teilerfremd zu n. Beweise:

c) $\operatorname{ind}_w(a \cdot b) \equiv \operatorname{ind}_w(a) + \operatorname{ind}_w(b) \pmod{\varphi(n)}$

d) $\operatorname{ind}_w(a^r) \equiv r \cdot \operatorname{ind}_w(a) \pmod{\varphi(n)} \quad (\forall\, r \in \mathbb{N})$

e) $\operatorname{ind}_w(-1) = \frac{1}{2}\varphi(n) \quad (n \geq 3)$

f) Ist v eine weitere Primitivwurzel modulo n, so gilt: $\operatorname{ind}_w(a) \equiv \operatorname{ind}_w(v) \cdot \operatorname{ind}_v(a) \pmod{\varphi(n)}$. (5)

32. Aufgabe: Sei p eine ungerade Primzahl und w eine Primitivwurzel modulo p^k $(k \in \mathbb{N})$. Beweise:

a) Ist w ungerade, so ist w auch eine Primitivwurzel modulo $2\,p^k$

b) Ist w gerade, so ist $w + p^k$ eine Primitivwurzel modulo $2\,p^k$

c) Die Anzahl der Primitivwurzeln modulo p^k ist gleich der Anzahl der Primitivwurzeln modulo $2\,p^k$. (3)

33. Aufgabe: a) Für $a \in \mathbb{Z}$ sei $k := \operatorname{ord}_n(a)$. Beweise, daß dann auch jede Zahl $b \in \mathbb{Z}$ mit $b \equiv a \pmod{n}$ modulo n die Ordnung k hat.

b) Beweise: Ist $w \in \mathbb{Z}$ eine Primitivwurzel modulo n, so ist auch jede Zahl $v \in \mathbb{Z}$ mit $v \equiv w \pmod{n}$ eine Primitivwurzel modulo n. (2)

34. Aufgabe: a) Bestimme die Anzahl der (inkongruenten) Primitivwurzeln modulo 375 bzw. 486.

b) Bestimme die kleinste positive Primitivwurzel w modulo 19 und den Index von $a \in \{6, -6, 14\}$ modulo 19 zur Basis w.

c) $v := 15$ ist ebenfalls eine Primitivwurzel modulo 19 (das muß nicht bewiesen werden!). Bestimme den Index von 6 modulo 19 zur Basis v und überprüfe an Hand dieses Beispiels die Aussage f) aus Aufgabe 31. (4)

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