6. Übungsblatt

ZAHLENTHEORIE (SS 2007)

Abgabe: Mi. 23.5.2007, 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!

21. Aufgabe: Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Beweise die Äquivalenz der folgenden Aussagen:

a) $\operatorname{ggT}(a, n) = 1$

b) Es existiert ein $k \in \mathbb{N}$ mit $a^k \equiv 1 \pmod{n}$. (2)

22. Aufgabe: Seien $a, b \in \mathbb{Z}$ und $n_1, n_2, \ldots, n_r \in \mathbb{N}$ $(r \geq 2)$.

a) Sei $k := \operatorname{kgV}(n_1, n_2, \ldots, n_r)$. Beweise:

$$a \equiv b \pmod{n_i} \quad (\forall\, i = 1, 2, \ldots, r) \quad \Longrightarrow \quad a \equiv b \pmod{k}$$

b) Welche Form hat das Ergebnis aus a) wenn man voraussetzt, daß die Zahlen $n_1, n_2, \ldots, n_r$ paarweise teilerfremd sind? Begründung! (2)

23. Aufgabe: Stelle nach der in der Vorlesung behandelten Methode eine Regel für die Teilbarkeit einer natürlichen Zahl a durch 16 auf und beweise diese. Benutze diese Regel, um zu prüfen, ob die Zahl 1 975 296 durch 16 teilbar ist.

b) Stelle eine Regel für die Teilbarkeit einer natürlichen Zahl a durch 176 auf und beweise diese. Benutze diese Regel, um zu prüfen, ob die Zahl 608 394 864 durch 176 teilbar ist. (3)

24. Aufgabe: Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, n) = 1$. Beweise:

a) a hat genau dann die Ordnung k modulo n, wenn die beiden folgenden Bedingungen erfüllt sind: **i)** $a^k \equiv 1 \pmod{n}$ und **ii)** $a^{\frac{k}{p}} \not\equiv 1 \pmod{n}$ für alle $p \in T_{\mathbf{P}}(k)$.

b) a hat genau dann die Ordnung $\varphi(n)$ modulo n, wenn gilt: $a^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$ für alle $p \in T_{\mathbf{P}}(\varphi(n))$.

c) Ist $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 1 \pmod{4}$ und $p \nmid a$ und gilt $\operatorname{ord}_p(a) = p - 1$, so folgt auch $\operatorname{ord}_p(-a) = p - 1$.

d) Untersuche, ob die Aussage in c) auch für alle Primzahlen p mit $p \equiv 3 \pmod{4}$ richtig ist. (5)

25. Aufgabe: Bestimme die kleinste positive Zahl $a \in \mathbb{Z}$ mit $\operatorname{ord}_{23}(a) = 22$. (2)

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