9. Übungsblatt

ZAHLENTHEORIE (SS 2007)

Abgabe: Mi. 13.6.2007, 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!

35. Aufgabe: Sei $m \in \mathbb{N}, m \geq 2$, und es sei $a \in \mathbb{Z}$ eine ungerade Zahl. Beweise:

a) Die Kongruenz $x^m \equiv a \pmod 2$ ist eindeutig lösbar.

b) Ist m ungerade, so ist die Kongruenz $(\star)$ $x^m \equiv a \pmod 4$ eindeutig lösbar.

c) Ist m gerade, so gilt:

i) $(\star)$ ist nicht lösbar, falls $a \equiv 3 \pmod 4$ gilt.

ii) $(\star)$ besitzt genau 2 Lösungen falls $a \equiv 1 \pmod 4$ gilt. (3)

36. Aufgabe: Bestimme alle Lösungen der Kongruenz $x^{12} \equiv 11 \pmod{19}$, die in $\{1, 2, \ldots, 18\}$ liegen (aber nicht durch stures Rechnen!). (3)

37. Aufgabe: a) Sei $w \in \mathbb{Z}$ eine Primitivwurzel modulo n. Die Zahlen $a, b \in \mathbb{Z}$ seien beide teilerfremd zu n. Beweise, daß die Kongruenz

$$(\star) \qquad a^x \equiv b \pmod n$$

genau dann lösbar ist, wenn $g := \mathrm{ggT}(\mathrm{ind}_w(a), \varphi(n))$ ein Teiler von $\mathrm{ind}_w(b)$ ist, und daß $(\star)$ im Falle der Lösbarkeit genau g Lösungen modulo $\varphi(n)$ hat.

b) Begründe, daß die Kongruenz $11^x \equiv 7 \pmod{19}$ lösbar ist und bestimme mit den Methoden von a) alle ihre Lösungen. (4)

38. Aufgabe: Bestimme alle Lösungen der folgenden Polynomkongruenzen (aber nicht durch stures Rechnen!)

a) $x^5 - 5x^3 + 11 \equiv 0 \pmod{294}$

b) $x^3 - 2x^2 + 1 \equiv 0 \pmod{55}$. (4)

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