Mathematisches Institut
Universität Münster
Priv.-Doz. Thilo Kuessner 10. Juni 2009

Algebra und Zahlentheorie, SS 2009, Probeklausur

Bearbeitungszeit: 80 Minuten

Aufgabe 1 Richtig oder Falsch (ankreuzen, je richtiger Aufgabe 1 Punkt, je falscher Aufgabe -1 Punkt)

a) $2^{30} \equiv 2 \; mod \; 31$
b) $\phi(49) = 36$
c) 978-3-7757-2212-2 ist eine korrekte ISBN
d) $6x \equiv 3 \; mod \; 10$ hat keine ganzzahligen Lösungen.

Aufgabe 2:

Berechnen Sie (es genügt die Lösung anzugeben, je Aufgabe 1 Punkt):

a) den Rest von 7^{40} bei Division durch 55
b) die Cäsar-Verschlüsselung von KLAUSUR

c) $\sum_{i=1}^{5} \phi(i)$

d) alle Lösungen von $3x \equiv 1 \bmod 5$.

Aufgabe 3: (je Aufgabe 2 Punkte):

a) Geben Sie die Verschlüsselungsfunktion f und die Entschlüsselungsfunktion f^{-1} des RSA-Verfahrens mit öffentlichem Schlüssel n, e an.
b) Beweisen Sie: wenn $ggT(x, n) = 1$, dann ist $f^{-1}(f(x)) \equiv x \; mod \; n$.

Aufgabe 4: Definieren Sie (je Aufgabe 1 Punkt):

a) die Eulersche ϕ-Funktion

b) neutrales Element einer Gruppe

c) Carmichael-Zahl

d) den Schlüsselaustausch nach Diffie-Hellman

Aufgabe 5 (8 Punkte) **RSA**

Sei $n = 143$ und $e = 17$ der öffentliche Schlüssel eines RSA-Teilnehmers.
a) Verschlüsseln Sie den Klartext 121.
b) Faktorisieren Sie n als Produkt von Primzahlen.
c) Bestimmen Sie $d \in \mathbb{N}$ mit $ed \equiv 1 \; mod \; \phi(n)$.
d) Entschlüsseln Sie den Geheimtext 11.

Aufgabe 6 (8 Punkte) **Zahlenkongruenzen**

A) Berechnen Sie den Rest von 13^{32} bei Division durch 17.
B) Berechnen Sie den Rest von 13^{46} bei Division durch 17.
C) Finden Sie alle ganzzahligen Lösungen von

$$x \equiv 3 \bmod 17$$

$$x \equiv 5 \bmod 11.$$

D) Formulieren Sie den Kleinen Satz von Fermat.

Abgabe 21. Juli 2009 **in der Vorlesung** (nicht in die Postkästen).