Zirkel 10b, Hausaufgaben vom 31.10.2007

(zum 14.11.2007)

Zahlentheorie 4:
RSA-Verfahren (Open Key - Verschlüsselung)

1. Seien p und q zwei verschiedene Primzahlen und a eine nicht durch p und q teilbare natürliche Zahl. Zeige

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

2. Finde eine ganze Zahl d, so dass

$$7d \equiv 1 \pmod{160}.$$

Hinweis: Benutze den erweiterten Euklidischen Algorithmus für $7x + 160y = 1$.

3. Die Daten der RSA-Kodierung sind (Bezeichnungen wie in der Vorlesung)

$$p = 17, q = 11, \quad \text{(geheim)}$$
$$N = 187, e = 7 \quad \text{(öffentlich)}.$$

Von einem Klienten habt ihr den verschlüsselten Geheimtext

$$C = 11$$

bekommen. Bitte entschüsseln.