Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2013
Übungsblatt 11

Verantwortlich für die Übungen:
Dr. Blaž Mramor (blaz.mramor@math.uni-freiburg.de)

1. **Kleiner Satz von Fermat**
   (a) Zeigen Sie mit Hilfe des kleinen Satzes von Fermat, dass 9 keine Primzahl ist.
   (b) Berechnen Sie $2013^{2012} \pmod{2011}$.

2. **RSA-Verfahren**
   Der folgende binäre Code enthält eine mit dem RSA-Verfahren verschlüsselte Nachricht
   $$(11101010101, 10010001011, 11011111011)$$
   oder dezimal geschrieben
   $$(1877, 1163, 1787).$$
   Der öffentliche Schlüssel ist $(N = 2773, e = 17)$.
   Ihnen ist die folgende Faktorisierung in Primzahlen bekannt:
   $$2773 = 47 \cdot 59.$$
   Die Nachricht ist ein Vektor
   $$A^e = (a_1^e \text{ mod N}, a_2^e \text{ mod N}, a_3^e \text{ mod N}).$$
   (a) Berechnen Sie $\varphi(N)$ und ein Inverses d, so dass $d \cdot e \equiv 1 \bmod \varphi(N)$.
   (b) Berechnen Sie
   $$A = (a_1 \text{ mod N}, a_2 \text{ mod N}, a_3 \text{ mod N})$$
   und schreiben die Nachricht. Der Text der Originalnachricht wurde wie folgt kodiert. Buchstaben wurden repräsentiert durch zweistellige Dezimalzahlen
   $$A = 01, B = 02, C = 03, ..., Z = 26.$$
   Dann werden zwei hintereinanderstehende Buchstaben als eine Zahl mit 4 Zahlzeichen dargestellt $(AA = 0101, AB = 0102, ...)$.

3. **Neuer ISBN-Code**
   Ein Vektor $(b_1, ..., b_{12}) \in (\mathbb{Z}/10\mathbb{Z})^{12}$ wird mit einem Vektor $(b_1, ..., b_{13}) \in (\mathbb{Z}/10\mathbb{Z})^{13}$ codiert, wobei b_{13} so ausgewählt wird, dass gilt
   $$b_1 + 3b_2 + b_3 + 3b_4 + ... + 3b_{12} + b_{13} \equiv 0 \text{ mod } 10.$$
   (a) Zeigen Sie, dass dieser Code einen Fehler erkennt.
   (b) Welche Vertauschungen von zwei nebeneinanderstehenden Ziffern werden erkannt?

Bitte wenden!

4. **Chinesischer Restsatz**

(a) Finden Sie (falls möglich) eine ganze Zahl z so, dass die folgenden Kongruenzen erfüllt sind:

$$\begin{aligned} z &\equiv 0 \mod 2 \\ z &\equiv 4 \mod 9 \\ z &\equiv 9 \mod 11 \end{aligned}$$

(b) Finden Sie (falls möglich) eine ganze Zahl z so, dass die folgenden Kongruenzen erfüllt sind:

$$\begin{aligned} 3 \cdot z &\equiv 4 \mod 5 \\ 5 \cdot z &\equiv 2 \mod 6 \\ 2 \cdot z &\equiv 3 \mod 7 \end{aligned}$$

Hinweis: Multiplizieren Sie zuerst jede Gleichung $a \cdot z \equiv b \mod c$ mit $a^{-1} \mod c$.

Abgabe am 8.7.2013 im Hörsaal vor Beginn der Vorlesung