Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2012

Übungsblatt 11

Verantwortlich für die Übungen:
Dr. Fritz Hörmann (fritz.hoermann@math.uni-freiburg.de)

1. **Chinesischer Restsatz** (6 Punkte).

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

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

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

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

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

   $$\begin{aligned} z &\equiv 1 \pmod 2 \\ z &\equiv 2 \pmod 9 \\ z &\equiv 7 \pmod{15} \end{aligned}$$

2. **RSA-Verfahren** (8 Punkte). Der folgende (hexadezimale) Code enthält eine mit dem RSA-Verfahren verschlüsselte Nachricht

   ```
   6cdaaa6c 6d70a7a1 bcbd6902 9463853c
   ```

   Der öffentliche Schlüssel ist $(N = 4\ 111\ 577\ 933, e = 63\ 139)$.

   Ihnen ist die folgende Faktorisierung in Primzahlen bekannt:

   $$4\ 111\ 577\ 933 = 62\ 731 \cdot 65\ 543.$$

   Berechnen Sie den privaten Schlüssel und dekodieren Sie die Nachricht.

   Der Text der Originalnachricht wurde wie folgt kodiert. Er wurde im ANSI/ASCII Zeichensatz repräsentiert und dann in Folgen aus 4 Zeichen zerlegt. Jede dieser Zeichenfolgen aus 4 Zeichen ergibt so eine Zahl x zwischen 0 und $2^{32} - 1$, die dann mit dem RSA-Verfahren mit öffentlichem Schlüssel $(N = 4\ 111\ 577\ 933, e = 63\ 139)$ codiert wurde, d. h. es wurde x^e modulo N berechnet. Bitte geben Sie alle Schritte Ihrer Rechnung an.

Bitte wenden!

3. **Multiplikative Ordnung** (4 Punkte). Sei N eine ganze Zahl und m eine zu N teilerfremde Zahl. Beweisen Sie: Es gibt eine ganze Zahl $n \geq 1$ so, dass

$$N|(m^n - 1).$$

Finden Sie jeweils das kleinste n für $m = 3, 5, 7$ und $N = 358$.

Hinweis: Überlegen Sie, welche n in Frage kommen, und potenzieren Sie möglichst effizient — siehe auch Aufgabe 4. 179 *und* 89 *sind prim.*

4. **Effizientes Potenzieren modulo** N (4 Punkte). Schreiben Sie eine Funktion (in einer Programmiersprache Ihrer Wahl), die effizient modulo N mittels „binärer Exponentiation“ potenziert. D. h. gegeben $N \in \mathbb{N}_{>0}$, $0 \leq x < N$ und $y \in \mathbb{N}$, berechne $0 \leq z < N$ so, dass

$$(\overline{x})^y = \overline{z}$$

in $\mathbb{Z}/N\mathbb{Z}$.

Die Funktion sollte für alle $N < \sqrt{b}$ korrekt sein, wobei b der verwendete Zahlbereich ist (also z.B. $b = 2^{64}$ bei der Verwendung von 64-Bit Zahlen).

Abgabe am 16.7.2012 im Hörsaal vor Beginn der Vorlesung