Nelius/Nöcker

10. Übungsblatt

MATHEMATIK FÜR INFORMATIKER I (WS 2000/01)

Abgabe: Montag, 15.1.2001 bis **13.00 Uhr !!!**

Internet–Adresse der Vorlesung:
http://math–www.uni–paderborn.de/~chris/index9.html

35. Aufgabe: Wie groß ist die Wahrscheinlichkeit, daß ein geordnetes Paar $(a, b) \in \{1, 2, \ldots, 10\} \times \{1, 2, \ldots, 10\}$ aus teilerfremden Zahlen a und b besteht? (Hinweis: Die Wahrscheinlichkeit eines Ereigneisses ist definiert als Quotient "Anzahl der günstigen Fälle" durch "Anzahl der möglichen Fälle") (3)

36. Aufgabe: Ein Bauer im Lippischen besitzt einen rechteckigen Acker. Dieser ist 143 Meter lang und 77 Meter breit. Besagter Bauer will diesen Acker rundherum einzäunen. Dazu will er so wenig Pfähle wie möglich verwenden. Alle Pfähle sollen denselben Abstand zueinander haben; hierbei sind nur ganze Meter als Abstand zulässig! Aus Stabilitätsgründen muss an jeder Ecke ein Pfahl eingeschlagen werden. Wieviele Pfähle braucht der Bauer mindestens? (3)

37. Aufgabe: Der *erweiterte Euklidische Algorithmus (EEA)* spielt bei einem der bekanntesten modernen Kryptographie-Verfahren, dem sogenannten *RSA-Verfahren*, eine zentrale Rolle. Ziel dieser Aufgabe ist es, einen ersten Eindruck von dieser Anwendung des EEA zu gewinnen.

1. Am Anfang des Verfahrens bestimmt man zwei (in der Praxis ca. 300 Dezimalstellen lange) Primzahlen p und q. Zeige, dass $p = 37$ und $q = 29$ Primzahlen sind, indem du begründest, dass diese Zahlen keine positiven Teiler außer 1 und sich selbst besitzen.

2. Berechne nun $N = p \cdot q$ und $M = (p-1) \cdot (q-1)$.

3. Zuerst wählt man eine Zahl $1 < e < M$, die teilerfremd zu M sein muss. Zeige mit Hilfe des euklidischen Algorithmus, dass die Wahl $e = 275$ diese Bedingung erfüllt.

4. Bestimme nun mit Hilfe des EEA zu $e = 275$ Zahlen $1 < d < M$ und $k \in \mathbb{Z}$, so dass gilt:

$$(\star) \qquad e \cdot d + k \cdot M = 1.$$

   Das Paar (e, N) ist nun der *öffentliche Schlüssel*, d. h., dass dieses Zahlenpaar jedem bekannt gegeben wird. Das Paar (d, N) hingegen birgt das für die Sicherheit des RSA-Systems wichtige Geheimnis und darf nur dem Erzeuger des Schlüssels bekannt sein. Man nennt dieses zweite Paar *privaten Schlüssel*. Die Zahlen M, p und q werden nach dem Errechnen der beiden Schlüsselpaare vernichtet!

5. Nachrichten werden vor ihrer Verschlüsselung in Zahlen umgewandelt. Um eine Nachricht $0 \leq m < N$ geheim zu übertragen, verwendet man den öffentlichen Schlüssel (e, N). Man berechnet dazu

$$y := m^e \bmod \mathrm{N}.$$

Die geheime Nachricht y ist dabei wieder eine Zahl zwischen 0 und $N - 1$. Diese Verschlüsselung kann jeder machen, da ja der öffentliche Schlüssel allgemein bekannt ist. Um die Entschlüsselung vorzunehmen, muss man den privaten Schlüssel (d, N) kennen, denn es gilt (Beweis s. 6.):

$$m = y^d \bmod \mathrm{N}.$$

Somit kann also jeder eine geheime Nachricht an den Erzeuger des öffentlichen Schlüssels schicken. Entschlüsseln kann diese aber nur der Besitzer des privaten Schlüssels!

Entschlüssele mit dem oben berechneten privaten Schlüssel die geheime Nachricht $y = 1006$. Diese ist zuvor mit dem öffentlichen Schlüssel (e, N) verschlüsselt worden. (7)

6. (ohne Wertung) Man kann natürlich beweisen, dass

$$(\star\star) \qquad (m^e)^d \bmod N = m$$

gilt. Dazu nutzt man die Tatsache, dass

$$(\star\star\star) \qquad m^M \bmod \mathrm{N} = 1$$

ist, falls m teilerfremd zu N ist. Zeige für teilerfremde Zahlen m und N, dass $(\star\star)$ gilt. Verwende dazu $(\star\star\star)$ und $(\star)$.

7. (ohne Wertung) Überlege dir, welcher Zusammenhang zwischen den beiden Zahlen M und N besteht.

38. Aufgabe: Wandle die Dezimalzahlen $a = 141$ und $b = 152$ in Zahlen zur Basis 4 um, addiere und multipliziere diese Zahlen in der Darstellung zur Basis 4 und überprüfe die Ergebnisse, indem du sie wieder in Dezimalzahlen umwandelst und mit den Dezimalzahlen $a+b$ bzw. $a \cdot b$ vergleichst. (3)