Feruzan Ay (ayferuzan@yahoo.de) **SS 2003**
Marco Kunze (makunze@cs.tu-berlin.de) **15. 6. 2003**
Sebastian Nowozin (nowozin@cs.tu-berlin.de)

Lösungen zum 4. Übungsblatt
Diskrete und strukturelle Mathematik für Informatiker

Lösung zu Aufgabe 1:

- Methode des ersten Organisators

  Diese Methode ist nicht sinnvoll, da die Zahlen zu klein sind. Wenn 14 Leute mehr oder weniger fehlen, fällt das nicht auf, da immer ganze Zweier-, bzw. Siebenergruppen fehlen.

- Methode des zweiten Organisators

  Diese Methode ist nicht sinnvoll, da $6|246$ ist. Somit kann nicht festegestellt werden, ob nicht ganze Reihen von 246 Pfadfindern fehlen, da insgesamt ja maximal 1440 fehlen dürfen.

Die gesuchte Lösung lässt sich also nur durch das Zusammenlegen der beiden Ergebnisse errechnen. Sei x die Anzahl der vorhandenen Pfadfinder.

$$\begin{aligned} x &= n \cdot 246 + 38 \\ x &= m \cdot 7 + 5 \end{aligned}$$

$$\begin{aligned} n \cdot 246 + 38 &= m \cdot 7 + 5 \\ n \cdot 246 + 33 &= m \cdot 7 \end{aligned}$$

Da m ganzzahlig ist, muss $(n \cdot 246 + 33) \bmod 7 = 0$ gelten. Da $33 \bmod 7 = 5$, folgt, dass $n \cdot 246 \bmod 7 = 2$ sein muss. Also gilt $n = 7 \cdot y + 2$.
Damit ergibt sich zusammen mit der ersten Gleichung:

$$x = 38 + (7n + 2) \cdot 246 = 1722n + 530$$

bzw.

$$n = \frac{x - 530}{1722}$$

Gesucht wird das ganzzahlige n zwischen den Werten für $x = 28800$ und $x = 27360$.

- Für $x = 28800$ ist $n = 16,4169$.
- Für $x = 27360$ ist $n = 15,5807$.

Folglich ist das gesuchte $n = 16$. Es sind $1722 \cdot 16 + 530 = 28082$ Pfadfinder in Berlin angekommen.

Lösung zu Aufgabe 2:

a) Da $30 \bmod 7 = 2$ würde sich der 13. eines Monats mit jedem Monat 2 Wochentage weiterschieben. Wenn also im Januar der 13. auf einem Montag ist, liegt er im Februar auf einem Mittwoch, etc.

   Wie leicht zu sehen ist, werden so innerhalb von sieben Monaten alle Wochentage einmal von einem 13. belegt. Somit gibt es jedes Jahr einen Freitag den 13. uh!

b) Da 28 mod $7 = 0$ würde entweder jeder 13. eines Monats auf einem Freitag liegen, oder es würde nie einen Freitag den 13. geben.

Lösung zu Aufgabe 3:

Wir zeigen zunächst eine Umformung von $2^{pq} - 1$ mit $p, q \in \mathbb{N}$:

$$2^{pq} - 1 = (2^p - 1) \cdot T$$

Um T zu bestimmen, führen wir eine Polynomdivision durch und erhalten:

$$T = (2^{pq} - 1) : (2^p - 1) = 2^{p(q-1)} + 2^{p(q-2)} + \ldots + 2^p + 1$$

Also ist T ganzzahlig und eindeutig für jedes $2^{pq} - 1$ bestimmbar.

Beweis der Aufgabe durch Widerspruch: Sei $2^n - 1$ Primzahl, aber n keine Primzahl. Wir zerlegen n in zwei beliebige Faktoren p, q. Es gilt: $2^n - 1 = 2^{pq} - 1 = (2^p - 1) \cdot T$. Dann wäre aber $2^n - 1$ teilbar durch $(2^p - 1)$. Dies steht im Widerspruch zur Annahme, dass $2^n - 1$ Primzahl ist. Also muss für jede Primzahl der Form $2^n - 1$ gelten: n ist Primzahl.
Der Umkehrschluss gilt jedoch nicht, wie ein Gegenbeispiel zeigt:

$$2^{23} - 1 \bmod 47 = 0$$

Lösung zu Aufgabe 4:

1. Die Entschlüsselung der Nachricht erfolgt in mehreren Schritten:

   (a) Umwandlung in Zahlenvektor. Sei N die Nachricht, damit ist:

   $$N = (12, 0, 15, 11, 10)$$

   (b) Für jeden Buchstaben wird die Entschlüsselungsgleichung des RSA Verfahrens angewendet:

   $$x = y^d \bmod m$$

   Wobei in der Aufgabenstellung $m = 26$ und $d = 5$ gegeben ist. y ist jeweils ein Ciphertext-Buchstabe, x der resultierende Klartext-Buchstabe.

   (c) Rückumwandlung des Zahlenvektors in Buchstaben.

2. Die Nachricht lautet: `MATHE`

3. Zuerst zerlegen wir m in Primfaktoren: $m = 26 = 2 \cdot 13$. Damit kennen wir die sonst schwer zu ermittelnden Primfaktoren p und q. Wir wissen, dass e und d mittels der Gleichung

   $$e \cdot d \equiv 1 \bmod (p - 1)(q - 1)$$

   ermittelt wurden. Daher muss gelten: $e \cdot d \equiv 1 \bmod 12$. Es lässt sich schnell ermitteln, dass für $d = 5$ automatisch $e = 5$ gelten muss, da $5 \cdot 5 \equiv 25 \equiv 1 \bmod 12$ ist. Also ist $e = 5$.

Lösung zu Aufgabe 5:

1. Da $p = 89$ und $q = 127$ folgt sofort $m = pq = 11303$. Weiter gilt: $\phi(m) = (p-1)(q-1) = 11088$. Wir wählen eine zu $\phi(m)$ relativ prime Zahl e mit $e = 7349$. Wir errechnen d durch Ausprobieren so, dass gilt:
$$ed \equiv 1 \bmod 11088$$
und erhalten $d = 5501$.

   Das System operiert auf Zahlen zwischen 0 und 11302 (inklusive). Sei x die Klartextzahl, y die resultierende Ciphertext-Zahl. Der öffentliche Schlüssel e und der Modulo Wert m werden an den Sender ausgeliefert, der geheime Schlüssel d verbleibt einzig und allein beim Empfänger. Die Operation des Systems gestaltet sich jetzt wie folgt:

   - Verschlüsseln
     Man erhält den Ciphertext-Wert y durch Einsetzen in die Gleichung:
     $$y = x^e \bmod m = x^{7349} \bmod 11303$$
   - Entschlüsseln
     Man erhält den Klartext-Wert x durch Einsetzen des Ciphertext-Wertes x in die Gleichung:
     $$x = y^d \bmod m = y^{5501} \bmod 11303$$

2. Um den geheimen Schlüssel d des Benutzers zu errechnen, reicht es die Gleichung
$$e \cdot d \equiv 1 \bmod 46620$$
zu lösen. Durch den Tipp in der Aufgabenstellung wissen wir, dass für d gelten muss:
$$d = \frac{8 \cdot 46620 + 1}{227} = 1643$$
Also ist der geheime Schlüssel $d = 1643$.

   (Mit Kenntnis von m könnte man sofort noch p und q errechnen: $m = pq = 223 \cdot 211 = 47053$).

Lösung zur Zusatzaufgabe:

1. Sei $c = d = 7$. Aufgrund der Bedingungen für das RSA System gilt:
$$c \cdot d \equiv 49 \equiv 1 \bmod (p-1)(q-1)$$
Daher muss $(p-1)(q-1) < 49$ ist. Es ergeben sich folgende mögliche Kombinationen (bis auf Vertauschung identische Lösungen sind nicht aufgeführt):

p	q
3	3
3	4
3	5
3	7
3	9
3	13
4	5
4	9
5	4
5	5
5	7
5	13
7	9

Da wir $m = pq$ mit $m \geq 26$ wünschen, wählen wir $p = 3$ und $q = 9$. Dann gilt für die Umwandlung von Klartext x in Chiffretext y:

$$y = x^7 \bmod 27$$

Umgekehrt gilt für die Dechiffrierung des Chiffretexts y in den Klartext x:

$$x = y^7 \bmod 27$$

2. (keine Lösung)